Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Swiss Government PKI

**NON CLASSIFICATO**

# Direttive per la registrazione dei certificati di classe B della Swiss Government PKI

## Direttive di registrazione della Swiss Government PKI per la LRA

V6.0, 01.11.2019

| | |
|---|---|
| **Classificazione*** | Non classificato |
| **Stato**** | Validato |
| **Nome del progetto** | |
| **Abbreviazione del progetto** | |
| **Numero del progetto** | |
| **Capoprogetto** | |
| **Committente** | Swiss Government PKI |
| **Autore** | Daniel Stich |
| **Iniziali** | StiD |
| **Elaborato da** | Daniel Stich, Jürgen Weber, Beatrice Metaj |
| **Verificato da** | Michael von Niederhäusern |
| **Autorizzato da** | PKI Management Board |
| **Distribuzione** | LRA-Officer, ispettori |
| **Doc_ID** | 0002-RV-Swiss Government PKI B Registrierrichtlinien LRA |
| **Breve descrizione** | |
| **Luogo di archiviazione** | Certified PKI |

* Non classificato, a uso interno, confidenziale

** In corso di elaborazione, in corso di verifica, validato, concluso

## Controllo delle modifiche, verifica, approvazione

| Versione | Data | Descrizione/Osservazioni | Collaboratore/Ruolo |
|---|---|---|---|
| 2.91 | 23.07.2010 | Sostituisce le versioni 2.x, nelle quali i certificati di classe A e B vengono trattati in un unico documento | Andreas Zürcher |
| 2.92 | | Semplificazione del testo e garanzia di coerenza con il documento «CP/CPS» e le liste di controllo munite di link alle direttive | Daniel Stich |
| 2.93 | | Integrazione dei risultati della revisione fatta con A. Zürcher | Daniel Stich |
| 2.94 | | Integrazione del feedback della sezione LZPPS del Centro soluzioni | Daniel Stich |
| 3.00 | 23.02.2012 | Versione finale | Daniel Stich |
| 3.01 | 23.04.2012 | Modifica delle regole per il PIN | Daniel Stich |
| 3.02 | 30.01.2013 | PDF nelle procedure con RIO e rilascio dei certificati, trasmissione elettronica firmata dei documenti nell'ambito della procedura con RIO, modifiche del login a 2 fattori sui sistemi client dell'Amministrazione federale | Daniel Stich |
| 3.03 | 22.04.2013 | Inserimento dei certificati di funzione<br>Modifica AdminPKI-> Swiss Government PKI<br>Modifica unità organizzativa dopo ON BIT | Tomaso Vasella |
| 3.04 | 11.09.2013 | Daniel Stich | |
| 3.05 | 15.01.2015 | Daniel Stich | Concretizzazione dell'identificazione per mezzo dei documenti d'identità |
| 4.00 | 24.03.2015 | Daniel Stich | Utilizzo del nuovo template, inserimento nel sistema di gestione dei documenti |
| 4.1 | 22.09.2016 | Daniel Stich | Adattamento a nuovi wizard, procedure e prestaged smart card |
| 4.2 | 24.05.2017 | Daniel Stich | Integrazione dei nuovi moduli e delle nuove liste di controllo |
| 4.3 | 29.08.2017 | Daniel Stich | Regolamentazione globale dell'archiviazione elettronica del registro e dei giustificativi. |
| 5.0 | 08.11.2017 | Daniel Stich | Nuova versione corretta e approvata |
| 5.1 | 15.05.2019 | Daniel Stich | Adeguamento dei requisiti CSP per gli stranieri ammessi provvisoriamente (permesso F)<br>Identificazione del richiedente secondo la procedura di deroga inerente al permesso F |
| 5.2 | 03.09.2019 | Beatrice Metaj | Diversi adeguamenti a seguito dell'esito delle verifiche |

| Versione | Data | Descrizione/Osservazioni | Collaboratore/Ruolo |
|---|---|---|---|
| 5.2 | 20.09.2019 | Beatrice Metaj | Integrazione degli adeguamenti nell'allegato B (moduli), nelle condizioni contrattuali e di utilizzo e nelle direttive |
| 5.3 | 14.10.2019 | Cornelia Enke, Daniel Stich, Beatrice Metaj | Input della ditta In&Out, revisione annuale |
| 6.0 | 01.11.2019 | PKI Management Board | Approvazione della nuova versione |

## Definizioni, acronimi e abbreviazioni

| Termine/Abbreviazione | Definizione |
|---|---|
| **Admin-Directory** | Admin-Directory è un elenco elettronico dell'Amministrazione federale in cui sono registrati, tra l'altro, i certificati di crittografia e gli elenchi dei certificati revocati, accessibili agli utenti finali. Si tratta di un elenco predisposto conformemente alla raccomandazione X.500 [18]. |
| **AdminPKI** | Vecchia denominazione della Swiss Government PKI. Spesso viene ancora utilizzata come sinonimo. |
| **Applicazione di registrazione (AR)** | Cfr. voce «Client LRA». |
| **Authority Revocation List (ARL)** | Elenco delle autorità di certificazione revocate che riporta i certificati rilasciati dalle CA di secondo livello revocati dall'autorità che rilascia i certificati radice (Root CA). |
| **Autorità di certificazione (CA)** | Organismo di fiducia incaricato di rilasciare e gestire certificati e di gestire gli elenchi dei certificati revocati in conformità con la raccomandazione X.509 [19]. Le CA responsabili del rilascio dei certificati di classe B sono comunemente chiamate «Swiss Government Enhanced CA 01» e «Swiss Government Enhanced CA 02». |
| **Certificate Policy / Certificate Practice Statement (CP/CPS)** | Documento che descrive le procedure di rilascio e gestione dei certificati rilasciati dalla CA interessata. |
| **Certificate Revocation List (CRL)** | Elenco dei certificati revocati che riporta i punti di serie dei certificati revocati prima della loro scadenza. L'elenco è aggiornato dall'autorità di certificazione. |
| **Certificate Service Provider (CSP)** | Fornitore di servizi di certificazione: organizzazione che gestisce un'infrastruttura PKI (ad es. Swiss Government PKI). |
| **Certificato** | Documento elettronico che contiene la chiave pubblica del suo titolare e altri dati che lo riguardano. L'informazione completa è firmata digitalmente mediante la chiave privata dell'autorità di certificazione che rilascia il certificato. Il formato è conforme alla raccomandazione X.509 [19]. |
| **Certificato di funzione di classe B** | Per ottenere un certificato di funzione è indispensabile possedere un account di amministratore o di test valido. Il richiedente deve presentarsi di persona presso un'autorità di registrazione locale e identificarsi presentando un documento di viaggio valido. Diversamente da quanto avviene per il certificato standard di classe B e il certificato per un account di test, per un account di amministratore viene rilasciato solo un certificato di autenticazione (su smart card o chiavetta USB). |
| **Certificato standard di classe B** | Prodotto standard della SG-PKI (cfr. pagina Intranet dell'UFIT sotto Produktdefinition, in tedesco e francese). I certificati consegnati vengono caricati su una non-prestaged smart card o su una chiavetta USB. |
| **Classi di certificati** | La SG-PKI rilascia certificati delle classi A, B, C e D tramite diverse CA dall'infrastruttura a chiave pubblica (PKI) nell'Amministrazione federale [16]. |
| **Client BAB** | Postazione di lavoro della Confederazione (UFIT). |
| **Client LRA** | Denominato in passato anche postazione LRA, questo termine designa l'hardware dedicato (laptop, desktop del PC, scanner, stampante)e i corrispondenti software (applicazione di registrazione, firewall, cifratura del disco ecc.) che i LRA-Officer utilizzano per il rilascio e la revoca dei certificati. |
| **Cross certificate** | Certificato che serve a creare un rapporto di fiducia tra due autorità di certificazione. È chiamato anche certificato incrociato. |
| **Dati di attivazione** | Dati che un utente deve inserire per attivare un modulo crittografico (ad es. smart card). Le chiavi private non fanno parte dei dati di attivazione. |

| Termine/Abbreviazione | Definizione |
|---|---|
| **Firma digitale** | Risultato della codifica di un messaggio con l'ausilio di un sistema crittografico che utilizza le chiavi in modo che il destinatario del messaggio possa capire:<br>1. se la chiave utilizzata per crittografare il messaggio è quella del firmatario;<br>2. se dopo la codifica il messaggio è stato modificato. |
| **ISIU** | Incaricato della sicurezza informatica dell'unità amministrativa. |
| **Key Recovery Agent (KRA)** | Utente con una speciale autorizzazione che lo abilita a eseguire il key recovery wizard. L'autorizzazione KRA è parte integrante della funzione del LRA-Officer. Su specifica richiesta può essere accordata anche ad altri collaboratori. |
| **Local Registration Authority (LRA)** | Autorità di registrazione locale: persona o organizzazione responsabile dell'identificazione e della verifica dell'autorizzazione di un richiedente o di un titolare di certificati. La LRA non firma né rilascia certificati, bensì esegue determinati compiti su mandato della CA. Tali compiti sono svolti dai LRA-Officer. Oltre che dell'hardware (laptop) e dei software (client LRA) utilizzati per l'elaborazione dei certificati, le LRA sono responsabili anche dei locali in cui vengono identificati i clienti, conservati i loro dossier, rilasciati i certificati e messi in funzione i computer della LRA (postazione LRA). Nel caso dei certificati regolamentati per le autorità, la LRA si trova all'interno dell'organizzazione SG-PKI. |
| **Local Registration Authority Officer (LRA-Officer)** | Persona che opera su mandato della SG e svolge i compiti che incombono alla LRA, ad esempio l'identificazione dei clienti, l'elaborazione o la revoca dei certificati. |
| **Non-prestaged smart card** | Smart card non sottoposta alla procedura di preconfigurazione della SG-PKI. Questa smart card è inizializzata automaticamente durante il rilascio dei certificati di classe A e le relative chiavi digitali sono generate direttamente nel chip. |
| **Object Identifier (OID)** | Identificativo numerico univoco attribuito a un oggetto o a una categoria di oggetti conformemente alle norme internazionali. |
| **ODIC** | Organo direzione informatica della Confederazione. |
| **Permesso F** | Permesso per stranieri ammessi provvisoriamente. L'ammissione provvisoria è concessa a persone il cui allontanamento dalla Svizzera si è rivelato inammissibile (violazione del diritto internazionale pubblico), non ragionevolmente esigibile (pericolo concreto per lo straniero) o impossibile (motivi tecnici legati all'esecuzione). |
| **Personal Identification Number (PIN)** | Codice che permette all'utente di identificarsi quando utilizza la propria smart card. |
| **Personal Unblock Key (PUK)** | Codice utilizzato per sbloccare una scheda bloccata impostare un nuovo PIN dopo la ripetuta immissione errata del PIN. |
| **PIN Reset User (PRU)** | Utente abilitato all'esecuzione del wizard per il reset (ripristino) del PIN sulla propria postazione di lavoro per conto di un'altra persona. Ogni utente può essere un PRU a condizione che la sua postazione di lavoro sia dotata di due lettori di smart card. |
| **Politica di sicurezza** | Insieme delle direttive e delle disposizioni adottate a seguito di un'analisi dei rischi. Lo scopo è ridurre i danni potenziali grazie a una serie di misure preventive e alla messa in atto di opportuni interventi atti a correggere le eventuali irregolarità. La politica di sicurezza serve a proteggere le risorse vitali del fornitore del servizio di certificazione. Le specifiche della politica di sicurezza definiscono il livello di sicurezza ottimale che dovrebbe essere garantito per un sistema d'informazione e per ogni componente dell'architettura di sicurezza. |

| Termine/Abbreviazione | Definizione |
|---|---|
| **Prestaged smart card** | Smart card che prima di essere utilizzate vengono sottoposte alla procedura di preconfigurazione della SG-PKI. La procedura prevede l'inizializzazione delle smart card, la dotazione delle stesse di 3 serie ognuna composta da 3 coppie di chiavi e nel renderle sicure con un PUK e un PIN. Il numero di serie della smart card viene registrato a livello centrale unitamente agli identificativi delle chiavi, alla chiave di crittografia, al PUK e al PIN. |
| **Pubblicazione (di un certificato)** | Il certificato viene messo a disposizione di terzi per consentire la crittografia di informazioni. |
| **Public Key Infrastruktur (PKI)** | Infrastruttura a chiave pubblica: insieme delle direttive, delle procedure, dei server, dei programmi e delle postazioni di lavoro utilizzati per gestire le chiavi e i relativi certificati. |
| **Registration Identification Officer (RIO)** | Ufficiale incaricato di effettuare l'identificazione personale del richiedente in base a un documento di viaggio valido e alla richiesta compilata (richiesta tramite RIO di una smart card per il rilascio di certificati di classe B). Il RIO si occupa anche di consegnare al richiedente una smart card preconfigurata, di copiare il documento d'identità sulla richiesta e di trasmettere al LRA-Officer committente per posta, corriere o come file scansionati e firmati allegati a una e-mail crittografata, il documento firmato, la lista di controllo e le «Condizioni contrattuali e di utilizzo per i certificati di classe B della Swiss Government PKI». Il RIO lavora sempre su mandato di un LRA-Officer specifico. |
| **Richiedente** | Il richiedente è una persona che presenta una richiesta di certificato. A rilascio avvenuto, la persona viene definita titolare del certificato. |
| **Rinnovo di un certificato** | Un certificato viene rinnovato su richiesta del suo titolare. La coppia di chiavi relative al certificato viene ridefinita. Al titolare del certificato viene quindi rilasciato un nuovo certificato. La ricertificazione successiva a una revoca non è considerata rinnovo. |
| **Root CA** | Autorità di certificazione suprema che rilascia, attraverso la firma della chiave, i certificati della CA subordinata (certificati radice). La root CA non rilascia certificati per gli utenti (leaf certificate). |
| **Swiss Government Enhanced CA 02** | La Swiss Government Enhanced CA 02 consente di rilasciare unicamente certificati dell'Amministrazione federale per smart card preconfigurate (prestaged). |
| **Swiss Government Enhanced CA 01** | La CA permette di rilasciare certificati di classe B standard e certificati di classe B preconfigurati per Cantoni e uffici che non fanno parte della 1ª e 2ª cerchia dell'Amministrazione federale. |
| **Swiss Government PKI (SG-PKI)** | (Già AdminPKI): infrastruttura dell'UFIT per le classi di certificati proposte come servizio standard (in passato identificato come prestazione trasversale). |
| **Titolare del certificato** | Collaboratore o unità amministrativa dell'Amministrazione federale o delle amministrazioni cantonali o comunali. Conformemente alla raccomandazione X.509, nel certificato le suddette amministrazioni sono denominate «subject» (soggetto). |
| **Utilizzatore del certificato** | Persona che utilizza un certificato di proprietà di un titolare. Può trattarsi anche di un'unità organizzativa dell'Amministrazione federale, un sistema informatico, un'applicazione informatica, il titolare di un certificato di un'altra PKI, un cliente o un fornitore. |

| Termine/Abbreviazione | Definizione |
|---|---|
| **Valore hash, fingerprint** | Valore numerico definito mediante l'utilizzo di un algoritmo detto «di hashing» sulla base di determinati dati inseriti. Poiché utilizzando un buon algoritmo si ottiene un valore hash diverso a fronte di dati diversi, tale valore serve tra le altre cose anche come «impronta digitale» per garantire la trasmissione inalterata di documenti. In caso di alterazione, il valore hash calcolato dal destinatario non coinciderebbe più con quello inviato dal mittente. Il valore hash crittografato con la chiave segreta del mittente viene designato firma digitale. |

## Documenti di riferimento

| Simbolo | Titolo, fonte |
|---|---|
| [1] | **Swiss Government PKI - Root CA I CP/CPS**<br>Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I<br>Versione V2.8 del 15.5.2019<br>Fonte: SG-PKI (http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf) |
| [2] | **Condizioni contrattuali e di utilizzo per i certificati di classe B**<br>Per i certificati personali e avanzati rilasciati dalla Swiss Government PKI delle autorità federali della Confederazione Svizzera<br>Versione 1.1 del 31.3.2017<br>Fonte: SG-PKI |
| [3] | **Linee guida della SG-PKI per i certificati di classe B**<br>Spiegazioni relative all'acquisizione e all'impiego di certificati di classe B della SG-PKI<br>Versione 1.0 del 9.3.2017<br>Fonte: SG-PKI |
| [4] | **Verifica dell'identità dei richiedenti di certificati di classe B**<br>Disposizioni vincolanti e dettagliate per verificare l'identità dei richiedenti di certificati di classe B della Swiss Government PKI, e relative deroghe<br>Versione 1.2 del 14.11.2017<br>Fonte: SG-PKI |
| [5] | **Modulo di richiesta complementare per i richiedenti con permesso F**<br>Documento da compilare in aggiunta al modulo di richiesta se il richiedente è sprovvisto di un documento di viaggio valido e se possiede soltanto un permesso F.<br>Versione 1.0 del 20.9.2019<br>Fonte: SG-PKI |
| [6] | **Quickguide WALK-IN SYNCHRON**<br>Guida rapida sul rilascio di certificati di classe B (standard e prestaged)<br>Versione 1.1 del gennaio 2017<br>Fonte: SG-PKI |
| [7] | **Quickguide PIN Reset**<br>Guida rapida sul reset del PIN della smart card per certificati di classe B (standard e prestaged)<br>Versione 1.1 del gennaio 2017<br>Fonte: SG-PKI |
| [8] | **Quickguide Rekeying (Renewal)**<br>Guida rapida sul rinnovo dei certificati di classe B (standard e prestaged)<br>Versione 1.1 del gennaio 2017<br>Fonte: SG-PKI |

| Simbolo | Titolo, fonte |
|---|---|
| [9] | **Quickguide Key Recovery**<br>Guida rapida sul ripristino dei certificati di crittografia di classe B (standard e prestaged)<br>Versione 1.1 del gennaio 2017<br>Fonte: SG-PKI |
| [10] | **Quickguide Revoke**<br>Guida rapida sulla revoca dei certificati prestaged di classe B<br>Versione 1.0 del 3.6.2016<br>Fonte: SG-PKI |
| [11] | **Quickguide Register Smartcard**<br>Guida rapida sulla registrazione della smart card<br>Versione 1.0 del 28.12.2016<br>Fonte: SG-PKI |
| [12] | **Quickguide cambio della lingua dei wizard**<br>Guida rapida per cambiare la lingua dei wizard<br>Versione 1.0 del 26.1.2017<br>Fonte: SG-PKI |
| [13] | **Direttive per il Registration Identification Officer (RIO)**<br>Versione V2.0 del 1.2.2014<br>Fonte: SG-PKI |
| [14] | **Quickguide WALK-IN ASYNCHRON**<br>Guida rapida sul rilascio di certificati di classe B (standard e prestaged) con RIO<br>Versione 1.1 del gennaio 2017<br>Fonte: SG-PKI |
| [15] | **Quickguide Token Unseal**<br>Guida rapida sullo sblocco di schede prestaged (rilascio tramite il RIO, guida gli utenti finali)<br>Versione 1.0 del 6.6.2016<br>Fonte: SG-PKI |
| [16] | Infrastruttura a chiave pubblica (PKI) nell'Amministrazione federale: documento di posizione e di strategia, versione 1.1 del 7.4.2004 |
| [17] | Ordinanza del 4.3.2011 sui controlli di sicurezza relativi alle persone (OCSP; RS 120.4)<br>Stato: 1° settembre 2017<br>Entrata in vigore: 1° aprile 2011<br>Fonte: https://www.admin.ch/opc/it/classified-compilation/20092321/201709010000/120.4.pdf |
| [18] | ITU-T X.500 – Repertorio standard: panoramica di programmi, modelli e servizi |
| [19] | ITU-T X.509 – Standard: dispositivo normativo per l'autenticazione |
| [20] | RFC 5280, Infrastruttura a chiave pubblica X.509 Internet, profili dei certificati e delle CRL; settembre 2005 |
| [21] | RFC 3647, Infrastruttura a chiave pubblica X.509 Internet, protocolli di gestione dei certificati; novembre 2003 |
| [22] | Istruzione tecnica n. 20 (DT20), Struttura dell'Admin-Directory, Ufficio federale dell'informatica e della telecomunicazione, 1.6.1999 |
| [23] | RFC 2526, Public Key Infrastructure Certificate Policy and Certificate Practices Framework, marzo 1999 |
| [24] | W002 - Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale |

| Simbolo | Titolo, fonte |
|---|---|
| [25] | Standard dell'ODIC «A006 – Smart card», versione 2.1 e relativo allegato (con i componenti autorizzati) |
| [26] | Enoncé des pratiques de certification de l'autorité de certification Admin-CA3, 30.3.2005 |
| [27] | Libro bianco concernente i requisiti di complessità per i codici PIN delle smart card<br>https://intranet.isb.admin.ch/dam/isb_kp/de/dokumente/themen/sicherheit/technologiebetrachtungen/ |
| [28] | Ordinanza del 22.2.2012 sul trattamento di dati personali derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione (RS *172.010.442*)<br>Stato: 1° aprile 2012<br>Entrata in vigore: 1° aprile 2012<br>Fonte: https://www.admin.ch/opc/it/official-compilation/2012/947.pdf |
| [29] | Legge federale del 19.6.1992 sulla protezione dei dati (LPD; RS *235.1*)<br>Stato: 1° marzo 2019<br>Entrata in vigore: 1° luglio 1993<br>Fonte: https://www.admin.ch/opc/it/classified-compilation/19920153/201903010000/235.1.pdf |
| [30] | Ordinanza del 4.7.2007 sulla protezione delle informazioni (OPrI; RS *510.411*)<br>Stato: 1° gennaio 2018<br>Entrata in vigore: 1° agosto 2007<br>Fonte: https://www.admin.ch/opc/it/official-compilation/2007/3401.pdf |
| [31] | Ordinanza del 9.12.2011 sull'informatica nell'Amministrazione federale (OIAF; RS *172.010.58*)<br>Stato: 1° aprile 2018<br>Entrata in vigore: 1° gennaio 2012<br>Fonte: https://www.admin.ch/opc/it/official-compilation/2011/6093.pdf |

# Indice

**Indice delle tabelle**

# 1 In generale

**Contenuto del documento**

Il presente documento contiene e descrive le direttive e le disposizioni applicabili al rilascio e alla gestione dei certificati di classe B della SG-PKI.

**Destinatari**

Il documento si rivolge principalmente ai LRA-Officer qualificati per il rilascio di certificati di classe B degli uffici pubblici e dei Cantoni. Serve all'organo di controllo esterno come quadro di riferimento per la verifica delle LRA nelle organizzazioni.

**Termini e abbreviazioni utilizzati**

I termini e le abbreviazioni utilizzati nel presente documento sono riassunti e spiegati in modo succinto nella tabella «Definizioni, acronimi e abbreviazioni».

**Documenti di riferimento**

I rimandi ai documenti di riferimento sono indicati con un numero posto tra parentesi quadre, ad esempio [1]. La pertinente tabella contiene un elenco di questi documenti, eventualmente corredato di informazioni supplementari (versione, fonte ecc.).

**Precisazione linguistica sull'uso del genere**

Per facilitare la lettura, i termini di genere maschile nel presente documento si riferiscono a persone di entrambi i sessi.

## 1.1 Oggetto del documento

Il documento «Swiss Government PKI - Root CA I CP/CPS» (di seguito «CP/CPS») [1] è il dispositivo normativo determinante per i certificati di classe B. Lo scopo del documento è definire i requisiti del CP/CPS riguardanti la LRA.

## 1.2 Campo di applicazione

La presente direttiva si applica a tutti i collaboratori che operano nell'ambito della LRA dei certificati di classe B. La SG-PKI può delegare i compiti della LRA della classe B ad altre unità organizzative che designeranno a loro volta i collaboratori esecutivi.

## 1.3 SG-PKI – certificati di classe B

**I certificati di classe B** sono salvati su un token di sicurezza (una smart card dotata di relativo criptochip) e vengono consegnati solo previa registrazione personale del richiedente.

Il titolare di un certificato di classe B è una persona fisica (non si tratta cioè di organizzazioni, gruppi o funzioni) e di regola detiene tre chiavi o una coppia di chiavi con i rispettivi certificati. A seconda del tipo di certificato (certificato standard di classe B o certificato di funzione di classe B), le chiavi sono tre (una per la firma, una per l'autenticazione e una per la crittografia delle chiavi e dei dati), oppure una sola (per l'autenticazione). Per i certificati di classe B prestaged, le smart card vengono fin dall'inizio preconfigurate con tre serie di tre coppie di chiavi ciascuna; di queste solo una serie viene associata contemporaneamente ai certificati attivi.

Per le organizzazioni che dispongono di un proprio sistema di gestione dei PUK, l'inizializzazione del token di sicurezza viene fatta con il tool fornito dal fornitore delle schede e non è parte integrante dell'applicazione di

registrazione. Le smart card che utilizzano il sistema di gestione dei PUK della SG-PKI vengono inizializzate durante la procedura di configurazione (prestaged smart card), direttamente al momento del loro rilascio con il walk-in wizard o register smartcard wizard (non-prestaged smart card).

Al momento del rinnovo, nel caso delle prestaged smart card la CA firma la terna di chiavi successiva, mentre nel caso delle non-prestaged smart card l'applicazione genera una nuova serie di coppie di chiavi che la CA provvederà a firmare. A quel punto, dalla scheda verranno eliminate solo le vecchie chiavi e i vecchi certificati usati per la firma e l'autenticazione. La vecchia coppia di chiavi per crittografare la chiave e i dati viene lasciata sulla scheda per una successiva decrittografia.

Un titolare può avere un certificato di classe A, un certificato di classe B standard/prestaged e uno o più certificati di funzione di classe B. **Non** è consentito archiviare i tre certificati summenzionati nel medesimo token di sicurezza, ma un token di sicurezza può contenere diversi certificati di funzione. Nel certificato, il/i nome/i e il/i cognome/i della persona devono essere chiaramente riconoscibili e visibili.

### 1.4 Token di sicurezza

Un elenco dei token di sicurezza supportati e le pertinenti direttive dettagliate figurano nello standard «A006 Smart card» [25] approvato dall'ODIC e nel relativo allegato.

# 2 Compiti del LRA-Officer e del RIO

## 2.1 Profilo dei requisiti del LRA-Officer

- assoluta integrità personale;
- metodo di lavoro preciso in base alle disposizioni della SG-PKI;
- affidabilità;
- attitudine al contatto con i clienti;
- disponibilità a esercitare un'attività costantemente tracciabile;
- disponibilità a sottoporsi a una verifica dell'affidabilità da parte della propria autorità, ad esempio a un controllo di sicurezza relativo alle persone secondo l'articolo 10 OCSP o a un controllo analogo (v. n. 3.12);
- divieto di inserire dati in Admin-Directory e di modificare quelli esistenti.

## 2.2 Compiti del LRA-Officer

Il LRA-Officer ha i compiti seguenti:

- verificare la richiesta nonché la documentazione e i moduli aggiuntivi necessari (v. n. 5.2.3.2);
- identificare il richiedente (v. n. 5.2.3.5 – Verificare l'identità del richiedente);
- verificare i dati in Admin-Directory;
- rilasciare i certificati;
- revocare i certificati;
- istruire i richiedenti in merito:
  - ✓ ai dati di attivazione;
  - ✓ alla protezione dei dati di attivazione;
  - ✓ ai loro diritti e obblighi;
  - ✓ alle «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2];
  - ✓ alle «Linee guida della SG-PKI per i certificati di classe B» [3];
- se del caso, compilare e archiviare liste di controllo;
- tenere un registro di tutte le attività che riguardano i certificati;
- gestire e conservare i dossier dei titolari dei certificati;
- gestire, eventualmente ordinare e se del caso inizializzare le smart card;
- garantire la formazione e la qualifica dei RIO;
- fornire ai RIO le copie dei moduli per la richiesta di un certificato di classe B con RIO, delle condizioni contrattuali e di utilizzo per i certificati di classe B, delle linee guida della SG-PKI per i certificati di classe B e della lista di controllo RIO;
- gestire l'elenco dei RIO;
- approvare le richieste di certificati nell'ambito delle procedure con RIO;
- tenersi aggiornati sulle disposizioni, sulle procedure e sugli strumenti tecnici riguardanti i certificati di classe B.

## 2.3 Profilo dei requisiti del RIO

- Capacità di lavorare con precisione seguendo le disposizioni della Swiss Government PKI e del LRA-Officer committente.

- Conoscenze di base del concetto di «tracciabilità» e comprensione della necessità di darvi attuazione nelle attività svolte in qualità di RIO.

### 2.4 Compiti del RIO

Il RIO tratta le richieste di certificati di classe B nel rispetto delle «Direttive per il Registration Identification Officer (RIO)» [13]. Al RIO competono i seguenti compiti:

- identificare i richiedenti;
- istruire i richiedenti in merito:
  - ✓ ai dati di attivazione;
  - ✓ alla protezione dei dati di attivazione;
  - ✓ ai loro diritti e obblighi;
- verificare la richiesta nonché la documentazione e i moduli aggiuntivi necessari (v. n. 5.2.3.2);
- fare una copia del documento d'identità e della richiesta;
- compilare la lista di controllo;
- inviare al LRA-Officer mandante per posta, corriere o posta elettronica la lista di controllo debitamente compilata, la copia firmata della richiesta, corredata di una copia del documento di viaggio valido e delle «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] debitamente firmate. Qualora si opti per la trasmissione elettronica di questi documenti, provvedere alla loro scansione in formato PDF, alla firma digitale dei file con il certificato di classe B personale e al loro invio al LRA-Officer per posta elettronica crittografata.

Un LRA-Officer può assumere il ruolo di RIO, ma non viceversa.

# 3 Aspetti operativi generali

## 3.1 Orari di servizio della LRA

Gli orari di servizio della LRA vengono stabiliti dalle unità organizzative responsabili.

## 3.2 Supporto della LRA

A supporto della LRA può intervenire il team operativo della SG PKI secondo le indicazioni del catalogo dei prodotti e servizi dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) o conformemente al service level agreement (SLA) in vigore.

In caso di guasti, il team operativo può essere contattato tramite il Service Desk UFIT, al recapito telefonico +41 (0)58 465 88 88.

Per domande e comunicazioni urgenti riguardanti la sicurezza, tramite il Service Desk UFIT, al recapito telefonico +41 (0)58 465 88 88, è possibile contattare anche un security officer della SG-PKI.

Per le domande e le notifiche meno urgenti riguardanti la sicurezza è possibile inviare un'e-mail all'indirizzo pki-secoff@bit.admin.ch. Per le ordinazioni e le domande di carattere generale, contattare direttamente il MAC-Manager-Team in MAC (Move/Add/Change) o il Service Desk UFIT, tel. +41 (0)58 465 88 88, in Service Request. La casella di posta elettronica pki-info@bit.admin.ch è disposizione come sempre per le richieste di consulenza e supporto.

## 3.3 Controllo dell'accesso ai locali della LRA

I locali della LRA non devono soddisfare requisiti particolari. Le attrezzature della LRA possono essere collocate in un normale ufficio. Tuttavia non possono essere utilizzati locali accessibili a persone non autorizzate (ad es. sale riunioni, infermerie o simili). I locali devono essere facilmente raggiungibili dai richiedenti e offrire loro una protezione della sfera privata sufficiente per permettere di inserire i codici (PIN e PUK) e le revoche delle passphrase. Se i collaboratori che ricoprono una funzione LRA lavorano insieme ad altri collaboratori in uffici open space, occorre predisporre uno spazio riservato alla funzione LRA adeguatamente protetto o munito di separatori. Il locale deve offrire possibilità sufficienti per tenere sottochiave il materiale della LRA, come moduli e dati dei clienti, come pure garantire una protezione della sfera privata sufficiente durante la procedura di rilascio dei certificati.

## 3.4 Controllo dell'accesso alla postazione e all'applicazione LRA

L'accesso al client della Confederazione (Bundesarbeitsplatz, BAB) con le funzioni del client LRA è protetto mediante l'autenticazione a due fattori (certificato di classe B). Il client LRA è dotato di un sistema di crittografia del disco rigido. È possibile attivare le applicazioni LRA soltanto con le autorizzazioni del LRA-Officer su un'altra scheda LRA-Officer, oppure su un normale certificato di classe B per l'autenticazione a due fattori. Altre persone, anche LRA-Officer, non possono accedere alle smart card personali con le autorizzazioni del LRA-Officer. Quando lascia la postazione BAB, il LRA-Officer deve sempre rimuovere la smart card dal lettore e conservarla sottochiave, oppure portarla con sé. Il PIN della smart card può essere annotato solo se conservato sottochiave e separatamente dalla smart card. Se si sospetta che un'altra persona ne sia venuta a conoscenza, il PIN deve essere cambiato immediatamente. L'eventuale perdita della smart card deve essere subito notificata al Service Desk UFIT e alla SG-PKI, che provvederanno a bloccarla immediatamente.

### 3.5 Policy riguardante i client LRA

Per i client BAB con funzione LRA e per i rispettivi utenti vigono rigorose prescrizioni di sicurezza, nonché le «W002 - Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale» [24] e le disposizioni dell'OIAF [31]. È severamente vietato:

- installare software di propria iniziativa;
- collegare hardware non forniti dall'UFIT;
- modificare la configurazione dell'hardware e dei software;
- utilizzare il client LRA per attività che esulano da quelle espressamente previste.

### 3.6 Moduli e dati dei clienti

È imperativo utilizzare i moduli elencati nelle presenti direttive ed emessi dalla SG-PKI, tranne che si faccia espresso riferimento ad alternative consentite (in formato cartaceo o elettronico). Per motivi di tracciabilità non è ammesso l'utilizzo di altri moduli o di soluzioni elettroniche.

I dossier dei clienti (moduli di richiesta, fogli informativi, richieste di revoca ecc.) devono essere conservati sotto chiave (principio «clear desk»). Il locale deve essere chiuso a chiave e accessibile solo al LRA-Officer, oppure i documenti devono essere riposti in un armadio chiuso a chiave a cui ha accesso solo il LRA-Officer.

Se i dossier dei clienti sono in formato elettronico, i dati devono essere salvati in un archivio a cui possono accedere solo le persone autorizzate, ossia il LRA-Officer e gli ispettori. Inoltre dovrà essere garantito il rispetto delle condizioni definite al numero 3.8. Tutti i giustificativi conservati in archivio devono essere disponibili in formato PDF/A e validamente firmati con il certificato di classe B del LRA-Officer competente o del RIO che ne ha fatto richiesta.

### 3.7 Registro

Nel registro devono essere annotate tutte le attività della LRA o importanti, ad esempio:

- il rilascio di certificati;
- la revoca di certificati;
- la sostituzione, la riparazione e lo spostamento temporaneo del client LRA;
- la ricezione di nuovi sbozzi di smart card;
- la ricezione di nuove smart card per i LRA-Officer;
- le richieste di reset del PIN (se non viene utilizzato il sistema della SG-PKI previsto a tale scopo);
- se del caso, numeri di mandato interni (ad es. il numero di ticket nel sistema di registrazione dei mandati).

Il LRA-Officer può tenere i registri in formato cartaceo (v. allegato «Registro della Swiss Government PKI per certificati di classe B») o elettronico. In quest'ultimo caso il LRA-Officer deve stampare, firmare e archiviare i registri ogni sera. In alternativa i registri in formato elettronico possono essere esportati giornalmente in un file PDF/A, firmati con il certificato di classe B del LRA-Officer e provvisti della marca temporale elettronica qualificata della SG-PKI del servizio TSA della SG-PKI (Time Stamping Authority della Swiss Government PKI, TSA). Di principio è consentito tenere più registri per ogni LRA (ad es. suddivisi per LRA-Officer, unità amministrativa, mese ecc.), a patto che la cronologia sia garantita in modo permanente. I dati del registro possono essere salvati localmente sul client LRA soltanto in via temporanea. In seguito bisogna trasferirli su un supporto che ne garantisca l'archiviazione conformemente alle indicazioni di cui al numero 3.8 e alle disposizioni della LPD, nonché che protegga tali dati dall'accesso da parte di terzi non autorizzati.

Nel registro devono essere annotate almeno le informazioni seguenti:

1. numero progressivo della registrazione;
2. data;
3. nome del LRA-Officer responsabile dell'esecuzione;
4. nome del cliente (richiedente/titolare del certificato);
5. tipo di attività (CS: certificato standard, CFA: certificato di funzione Admin, CFT: certificato di funzione test, RI: rilascio, RE: revoca, K: Key Recovery, PR: PIN Reset).

### 3.8 Termini di conservazione

I moduli, i dati dei clienti e i registri di cui ai numeri 3.6 e 3.7 devono essere conservati in ogni caso per almeno 11 anni dopo la scadenza della validità del rispettivo certificato. In questo periodo di tempo gli ispettori devono poter accedere all'archivio. L'accesso protetto riguardante questi dati deve essere assicurato anche per i dossier di clienti tenuti in formato elettronico (ossia accesso consentito esclusivamente ai LRA-Officer e negato a tutti gli altri).

### 3.9 Conservazione delle smart card vergini

Le smart card vergini, registrate e preconfigurate e gli altri supporti dati sensibili devono essere conservati in un luogo sicuro. Le smart card devono essere conservate in un locale chiuso a chiave accessibile soltanto ai LRA-Officer oppure sottochiave in un armadio le cui chiavi sono disponibili soltanto ai LRA-Officer.

### 3.10 Utilizzo di certificati con autorizzazioni di LRA-Officer e relativa protezione

I certificati con autorizzazioni di LRA-Officer devono essere utilizzati solo per gli scopi previsti e non possono essere trasferiti a terzi. I LRA-Officer devono proteggere le loro chiavi private/i loro certificati privati sulla smart card con i dati di attivazione come indicato al numero 3.4.

### 3.11 Smaltimento

I documenti cartacei non più necessari riguardanti la LRA (direttive, liste di controllo, appunti ecc.) o i clienti (richieste di partecipanti, elenchi ecc.) devono essere distrutti con un tritacarte o gettati in un contenitore di sicurezza per poi essere smaltiti. Prima di smaltirle o distruggerle, le smart card non più utilizzate devono essere forate con una perforatrice.

Eventuali guasti al BAB client devono essere notificati al Service Desk UFIT.

### 3.12 Verifica dell'affidabilità

Prima di candidarsi al ruolo di LRA-Officer, l'autorità prende le misure ragionevolmente esigibili e consentite dalla legge per accertare l'affidabilità e l'integrità del candidato. La SG-PKI raccomanda all'autorità di adottare le seguenti misure:

- il controllo di sicurezza di base secondo l'articolo 10 OCSP [17] presso il servizio specializzato per i controlli di sicurezza relativi alle persone in seno al Dipartimento federale della difesa, della protezione della popolazione e dello sport (servizio specializzato CSP DDPS);

e/o

- adozione di misure proprie per verificare l'affidabilità, ad esempio:
    - ✓ il controllo dell'identità del candidato (passaporto o carta d'identità);
    - ✓ la verifica di referenze professionali e private del candidato;

- ✓ la verifica della completezza e coerenza del curriculum vitae del candidato;
- ✓ il controllo delle qualifiche accademiche e professionali dichiarate;
- ✓ la verifica degli estratti dal registro delle esecuzioni e dal casellario giudiziale.

Il funzionario con potere di firma dell'autorità conferma alla SG-PKI l'affidabilità del candidato conformemente alla summenzionata raccomandazione o di aver effettuato la verifica in modo analogo. Una volta terminata la verifica, il funzionario giudica il candidato affidabile, integro e accerta che egli possieda le competenze necessarie esercitare la funzione di LRA-Officer, sensibile sotto il profilo della sicurezza.

### 3.13 Riservatezza, protezione dei dati

Il LRA-Officer è tenuto a firmare una dichiarazione di confidenzialità, che è parte del modulo di richiesta.

La LPD [29], l'ordinanza del 14 giugno 1993 sulla protezione dei dati (OLPD; RS *235.11*) e l'OPrl [30] devono essere rispettate.

In particolare è necessario che le informazioni concernenti clienti o dati importanti della LRA o della CA siano trasmesse in forma crittografata e rese inaccessibili agli utenti non autorizzati.

### 3.14 Formazione del personale

Tutti i LRA-Officer devono assolvere una formazione. Al termine della formazione un esame scritto permette di stabilire se il partecipante possiede conoscenze e competenze sufficienti per poter operare in veste di LRA-Officer per i certificati di classe B.

Se il candidato non supera l'esame, non riceve le autorizzazioni di LRA-Officer. Può però frequentare di nuovo il corso e ripetere l'esame, in modo da comprovare l'idoneità e le competenze necessarie. Se un LRA-Officer riscontra delle lacune nelle proprie conoscenze e competenze o se alcuni punti non gli sono chiari e non è in grado di ovviarvi personalmente, è tenuto a comunicarlo alla SG-PKI, e insieme cercheranno una soluzione.

In caso di violazioni delle direttive per la registrazione, la SG-PKI può bloccare i certificati del LRA-Officer e impedire così il rilascio di altri certificati per gli utenti finali.

Anche i RIO devono assolvere una formazione, ma di portata più limitata. In linea di massima tale formazione è impartita dal LRA-Officer incaricato, ma può anche essere impartita dalla SG-PKI. La formazione deve vertere come minimo sui seguenti documenti di riferimento: «Verifica dell'identità dei richiedenti di certificati di classe B» [13] ,«Direttive per il Registration Identification Officer (RIO)» [13] e «Linee guida della SG-PKI per i certificati di classe B»[3].

### 3.15 Aggiornamento della formazione

I LRA-Officer hanno l'obbligo di tenersi sempre aggiornati, in particolare sulle direttive di registrazione. A tal fine la SG-PKI mette a disposizione i documenti e le informazioni aggiornati nell'area riservata ai clienti della pagina Internet http://www.pki.admin.ch. Inoltre si impegna a notificare per e-mail eventuali modifiche importanti. A sua volta, i LRA-Officer che ricevono un'e-mail da parte della SG-PKI sono tenuti a leggere le informazioni al riguardo pubblicate nell'area riservata ai clienti della pagina Internet della SG-PKI.

Inoltre, i LRA-Officer sono tenuti a conseguire 20 punti in eventi di formazione continua su un periodo di osservazione di 18 mesi. La tabella indicata di seguito riporta il punteggio conseguibile per ogni tipologia di evento formativo:

| Evento formativo | Punteggio |
|---|---|
| Formazione di base | 10 |
| Formazione di base sul testing | 10 |
| Incontro dei LRA-Officer (mezza giornata) | 10 |
| Workshop per i LRA-Officer (mezza giornata) | 5–10<br>(a seconda del contenuto) |
| Workshop per i LRA-Officer ad hoc (min. 4 partecipanti, in loco) | 5–10<br>(a seconda del contenuto) |
| Riunione, teleconferenza (in funzione della tematica) | 5 |

Tabella 1: punteggio conseguibile dai LRA-Officer per evento formativo

La SG-PKI offre corsi di formazione e formazione continua per LRA-Officer a cadenza regolare (workshop, incontri). Se hanno conseguito un punteggio troppo basso, i LRA-Officer possono essere obbligati a seguire uno o più eventi formativi, a pena di revoca dell'autorizzazione per esercitare questa funzione. Il punteggio aggiornato può essere richiesto alla SG-PKI all'indirizzo pki-info@bit.admin.ch. La SG-PKI non pubblica alcun elenco al riguardo.

### 3.16 Regole per i PIN

I titolari di certificati utilizzano dei codici PIN (password) per attivare le loro schede con chip o le loro chiavi private. In linea di principio questo PIN è diverso dalla password che viene usata ad esempio per effettuare il login alle applicazioni [27]. Ogni titolare può scegliere il proprio PIN. Le regole che si applicano ai PIN per le smart card sono le seguenti:

- *lunghezza:* il PIN deve essere costituito da almeno 6 caratteri;
- *numero di tentativi:* la scheda deve bloccarsi automaticamente dopo al massimo 5 tentativi errati;
- *complessità:* i caratteri che compongono il PIN possono essere scelti liberamente (è consentito anche un codice totalmente numerico). È vietato utilizzare codici PIN banali (p. es. la propria ID utente oppure 123456);
- *validità:* il PIN deve essere immediatamente cambiato se si sospetta che qualcuno ne è venuto a conoscenza. Quando il ciclo di vita della smart card giunge al termine, per la nuova bisogna scegliere un nuovo PIN;
- *unicità:* il PIN deve essere utilizzato per una sola smart card.

Poiché la disposizione dei tasti sulla tastiera cambia secondo la lingua, è meglio non utilizzare caratteri speciali.

### 3.17 Passphrase di revoca

La passphrase di revoca serve a identificare l'utente durante una conversazione telefonica con il LRA-Officer, ad esempio in caso di richiesta di revoca dei suoi certificati o qualora si chieda al service desk competente di avviare il reset del PIN. La passphrase di revoca consiste in una domanda e nella corrispondente risposta.

Per la passphrase valgono due regole: le informazioni contenute nella passphrase devono essere tali da non poter essere desunte o facilmente indovinate da altre persone; il richiedente deve conoscere la passphrase in modo da essere sempre in grado di rispondere alle domande senza difficoltà o dubbi.

### 3.18 Reset del PIN e gestione del PUK

In linea di principio, per ogni smart card bloccata deve essere disponibile una procedura di sblocco tramite codice PUK. L'amministrazione del PUK rientra nell'ambito di competenze delle autorità, a meno che non venga utilizzata la carta prestaged della SG-PKI. Per le proprie carte prestaged, la SG-PKI ha sviluppato un sistema

elettronico centralizzato con amministrazione dei codici PUK. In questo sistema il codice PUK crittografato è memorizzato in uno dei server della SG-PKI. La procedura di sblocco della carta avviene in background.

Se per l'amministrazione del PUK di carte non prestaged è utilizzato un sistema alternativo (Scamiad, PrivacyPUK o altri), l'Ufficio deve provvedere affinché:

- soltanto le persone autorizzate (collaboratori dei service desk, LRA-Officer) dispongano dei PUK, sia in forma elettronica che scritta (su un foglio di carta, una busta ecc.);
- i LRA-Officer o il service desk competente possano accedere ai PUK soltanto previo espresso consenso dei titolari della carta (a causa della carta bloccata, ad es.);
- l'accesso ai PUK sia documentato in maniera chiara e comprensibile (ad es. mediante un sistema di registrazione dei mandati, di ticketing, un'annotazione nel registro ecc.);
- lo stesso PUK non sia utilizzato per più carte;
- i codici PUK non siano identificabili (ad es. attraverso il numero personale, il numero della carta ecc.);
- sia disponibile una descrizione esaustiva del sistema utilizzato (procedura, attività, ruoli, luoghi di archiviazione ecc.) approvata dall'Ufficio.

Se viene utilizzata una carta prestaged della SG-PKI, per il supporto del personale o i LRA-Officer valgono i principi indicati di seguito.

- Per effettuare il reset del PIN bisogna avere un superuser addetto a questa operazione. Il superuser può aprire un ticket interno per la carta tramite un'applicazione web, una volta identificato il titolare. L'identificazione può avvenire anche per telefono mediante la passphrase di revoca. Solo a quel punto il titolare della carta può ripristinare il proprio PIN con la funzione PRU.
- Per sbloccare la carta bisogna attivare la funzione PRU, il cui unico scopo è «prestare» il proprio PC al titolare e aprire per lui il PIN Reset wizard (visto che il titolare, avendo la carta bloccata, non può procedere all'autenticazione a due fattori al PC). Per attivare la funzione PRU l'utente interessato deve recarsi sul posto e inserire la propria carta in un secondo lettore nel PC previsto a questo scopo.
- Le funzioni del superuser addetto al reset del PIN e la funzione PRU non possono essere espletate dalla stessa persona. Le autorizzazioni si escludono a vicenda per rispettare il principio del doppio controllo della procedura di ripristino del PIN.

La procedura di ripristino del PIN per le carte prestaged è descritta in modo dettagliato nel documento «Quickguide: PIN Reset» [7].

## 4 Verifica di conformità

La SG-PKI è tenuta a verificare l'attuazione del CPS ogni 18 mesi. In particolare deve verificare l'osservanza delle presenti direttive da parte del LRA-Officer. La verifica di conformità può essere effettuata direttamente dalla SG-PKI o da un organo esterno da essa incaricato. I LRA-Officer sono tenuti a collaborare ai lavori di verifica e ad accordare l'accesso a procedure e documenti.

In caso di mancato superamento della verifica di conformità, il LRA-Officer può perdere l'autorizzazione. Se vengono rilevate lacune gravi, il responsabile PKI o della sicurezza SG-PKI può anche ordinare la revoca di tutti i certificati utente rilasciati dal LRA-Officer in questione.

# 5 Procedure della SG-PKI per i certificati di classe B

## 5.1 Panoramica

Esistono diversi tipi di certificati di classe B. Le tabelle sottostanti offrono una panoramica delle procedure applicabili ai certificati regolamentati per le autorità.

| Certificati di classe B caricati su smart card prestaged |
|---|
| La smart card è inizializzata presso la SG-PKI durante la procedura di preconfigurazione. |
| Nella procedura di preconfigurazione sono generate esternamente tre serie, composte di tre coppie di chiavi (firma, autenticazione, crittografia) ciascuna, e scritte sulla scheda. |
| Non è possibile effettuare il key recovery su una scheda che non appartiene al legittimo titolare (procura). |
| È possibile effettuare il key recovery della chiave di crittografia. |
| È possibile effettuare la procedura RIO. |
| La chiave può essere rinnovata (rekeying) per due volte al massimo. |

Tabella 2: procedura per i certificati di classe B caricati su smart card prestaged

| Certificati di classe B caricati su smart card non-prestaged |
|---|
| La smart card è inizializzata:<br>• al momento del rilascio dei certificati con il walk-in wizard;<br>• al momento della registrazione della smart card con il register smart card wizard; o<br>• dal LRA-Officer al di fuori della procedura, mediante un sistema di gestione dei PUK specifico dell'organizzazione. |
| Nella procedura di rilascio dei certificati sono generate tre coppie di chiavi (firma, autenticazione, crittografia) sulla scheda. |
| Non è possibile effettuare il key recovery (recupero della chiave) su una scheda che non appartiene al legittimo titolare (procura). |
| È possibile effettuare il key recovery della chiave di crittografia privata. |
| È possibile effettuare la procedura RIO. |
| Per ciascuna smart card, la chiave può essere rinnovata (rekeying) per due volte al massimo. |

Tabella 3: procedura per i certificati di classe B caricati su smart card non-prestaged

| Certificati di funzione di classe B per account di amministratore |
|---|
| La smart card è inizializzata dal LRA-Officer con il walk-in wizard dal momento del rilascio del certificato. |
| Nella procedura di rilascio, è generata soltanto la coppia di chiavi per l'autenticazione sulla scheda. |
| Non è possibile effettuare il key recovery su una terza chiave (procura). |
| Non è possibile effettuare il key recovery della chiave di autenticazione privata. |
| Non è prevista alcuna procedura RIO. |
| Il rinnovo non è consentito. |

Tabella 4: procedura per i certificati di funzione di classe B per account di amministratore

| Certificati di funzione di classe B per account di test |
|---|
| La smart card è inizializzata dal LRA-Officer con il walk-in wizard dal momento del rilascio del certificato. |
| Di regola, nella procedura di rilascio è generata una coppia di chiavi per l'autenticazione sulla scheda. All'occorrenza è consentito anche generare una chiave di firma e una di crittografia. |
| Non è possibile effettuare il key recovery su una terza chiave (procura). |
| È possibile effettuare il key recovery della chiave di crittografia privata. |
| È possibile effettuare la procedura RIO. |
| Il rinnovo non è consentito. |

Tabella 5: procedura per i certificati di funzione di classe B per account di test

Per le procedure con e senza RIO, il LRA-Officer e il partecipante hanno a disposizione diversi wizard. Al riguardo si rinvia ai documenti di riferimento [6], [7], [8], [9], [10], [11], [12], [14] e [15].

### 5.2 Procedura di rilascio dei certificati

Esistono due tipi di procedure di rilascio dei certificati:

- la procedura di rilascio senza RIO;
- la procedura di rilascio con RIO.

Di seguito le due varianti sono denominate semplicemente «rilascio senza RIO» e «rilascio con RIO».

Le differenze sono descritte nella tabella sottostante.

| Rilascio senza RIO | Rilascio con RIO |
|---|---|
| Il LRA-Officer provvede all'identificazione personale del richiedente. Per confermare l'avvenuta identificazione, il LRA-Officer scansiona il documento di viaggio valido del richiedente.<br>Per i richiedenti che sottostanno a disposizioni derogatorie, i documenti definiti nella pertinente deroga devono essere controllati e scansionati. Il modulo e la documentazione aggiuntiva richiesti per ciascun caso di deroga sono descritti al n. 5.2.3.5. | Il RIO provvede all'identificazione personale del richiedente. Per confermare l'avvenuta identificazione, il RIO fa una copia del documento di viaggio valido e del modulo di richiesta correttamente compilato.<br>Per i richiedenti che sottostanno a disposizioni derogatorie, i documenti definiti nella pertinente deroga devono essere controllati e scansionati. Il modulo e la documentazione aggiuntiva richiesti per ciascun caso di deroga sono descritti al n. 5.2.3.5.<br>Il RIO compila la lista di controllo e trasmette questi documenti, unitamente alle «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] debitamente firmate, al LRA-Officer per conto del quale opera. |
| Verifica del richiedente in Admin-Directory da parte del LRA-Officer. | Verifica del richiedente in Admin-Directory da parte del RIO. |
| Il LRA-Officer istruisce il richiedente sui dati di attivazione e sulla loro protezione. | Il RIO istruisce il richiedente sui dati di attivazione e sulla loro protezione. |
| Il LRA-Officer genera una richiesta per conto del richiedente. Nell'ultima fase del walk-in wizard, il LRA-Officer inserisce il suo codice PIN e i dati personali necessari per la revoca telefonica (passphrase di revoca). | Il LRA-Officer approva la richiesta. |

| Rilascio senza RIO | Rilascio con RIO |
|---|---|
| | Il richiedente inserisce il suo codice PIN e i dati personali necessari per la revoca telefonica (passphrase di revoca) al momento della rimozione del sigillo della smart card utilizzando l'unseal-wizard. |

Tabella 6: differenze con e senza RIO

### 5.2.1 Unità organizzative e collaboratori autorizzati a richiedere un certificato

Nella richiesta di autorizzazione quale LRA-Officer, la linea gerarchica stabilisce per quali unità organizzative e collaboratori possono essere rilasciati certificati. L'appartenenza del richiedente a una determinata unità organizzativa deve coincidere con l'autorizzazione di LRA-Officer. Ciò significa che all'interno dell'Admin-Directory il richiedente deve essere registrato nella stessa directory per la quale il LRA-Officer è stato abilitato. Altrimenti detto: le directory autorizzate devono essere registrate nell'account del LRA-Officer.

### 5.2.2 Modalità per la richiesta di un certificato

Il LRA-Officer o il responsabile PKI definisce le modalità per la richiesta di un certificato (per iscritto mediante modulo, Remedy-MAC ecc.). L'ordine deve essere tracciabile, ossia documentabile anche dopo 11 anni dalla scadenza del certificato La SG-PKI mette a disposizione un modulo che contiene tutti i dati necessari per la richiesta (v. allegato).

**NON CLASSIFICATO**

## Modulo di richiesta per il rilascio dei certificati personali di classe B della Swiss Government PKI

### Certificati avanzati

V2.3, 20.09.2019

Il presente modulo serve per richiedere un certificato di classe B della Swiss Government PKI. Si opera una distinzione tra i certificati standard (con autenticazione, firma e crittografia) e i certificati di funzione per account di amministratore e account di test (per i primi solo autenticazione).

**Per l'identificazione presso l'autorità di registrazione occorre una carta d'identità valida o un passaporto valido.**

** Campi obbligatori*

| | |
|---|---|
| Cognome e nome/i*: | |
| N. documento d'identità*: | Valido fino a*: |
| Unità organizzativa*: | |
| Tipo di certificato*: certificato di classe B standard | |
| E-mail*: | |
| Indirizzo aziendale*: | |
| Luogo d'origine: | Data di nascita: |
| N. smart card: | |

**Luogo e data*:** **Firma*:**

_____ _____

Se la richiesta di un certificato riguarda un caso di deroga (ad es. il richiedente possiede soltanto un permesso F), per tale deroga è imperativo compilare, senza eccezioni, la documentazione complementare della SG-PKI prevista a tale scopo e allegarla alla richiesta.

### 5.2.3 Rilascio senza RIO

Nello svolgimento delle proprie attività, la LRA utilizza i documenti di formazione del LRA-Officer e le guide rapide ai singoli wizard [6], [7], [8], [9], [10], [11], [12], [14] e [15]. In caso di indicazioni contraddittorie si applicano le presenti direttive.

Il LRA-Officer procede seguendo la «Lista di controllo per il rilascio dei certificati di classe B».

#### 5.2.3.1 Verifica dei dati in Admin-Directory

Affinché gli possa essere rilasciato un certificato, il richiedente deve essere registrato in Admin-Directory.

Al proposito devono essere soddisfatte le condizioni elencate di seguito.

1. Il campo «e-mail» deve contenere un indirizzo e-mail completo e plausibile.
   Nel caso di un certificato di funzione per account di amministratore: indirizzo e-mail del titolare dell'account.
   Nel caso di un certificato di funzione per account di test: l'indirizzo e-mail dell'account di test.
   L'indirizzo e-mail deve essere identificabile mediante il suffisso «test», «TST» o similare.
2. In presenza di più registrazioni: la registrazione per la quale deve essere rilasciato il certificato deve essere identificabile in maniera univoca tramite il suffisso del nome.

Se il richiedente non compare in Admin-Directory o compare in modo errato, l'amministratore di Admin-Directory presso l'Ufficio deve predisporne la registrazione o la modifica dei dati. La procedura di rilascio può essere ripresa soltanto a correzione avvenuta in Admin-Directory (in generale la replica dei dati dura almeno una notte). Il LRA-Officer può controllare l'operazione tramite, ad esempio, il walk-in wizard.

#### 5.2.3.2 Verifica del modulo di richiesta

Verificare che il modulo di richiesta sia completo e corretto con l'ausilio delle domande sottostanti.

1. Il richiedente è autorizzato secondo il numero 5.2.1 a presentare una richiesta a questo LRA-Officer?
2. I dati del richiedente indicati sul modulo coincidono con quelli registrati in Admin-Directory?
3. Il modulo è firmato e datato correttamente?

Dall'introduzione del login a due fattori per i client della Confederazione, i servizi RU competenti possono inviare al LRA-Officer l'elenco dei nuovi collaboratori anziché presentare singole richieste. Per ogni collaboratore l'elenco deve contenere gli stessi dati del modulo di richiesta. L'UFIT dispone internamente di un Remedy-MAC per l'ordinazione di certificati di classe B.

#### 5.2.3.3 Appuntamento per il rilascio del certificato

Per il rilascio del certificato deve essere fissato un appuntamento con il richiedente inviando un'e-mail all'indirizzo indicato sulla richiesta con il seguente contenuto:

1. proporre al richiedente una o più date per l'appuntamento;
2. invitarlo a presentarsi con un documento di viaggio valido che non risulti scaduto al momento della registrazione. Se sottostà alle disposizioni derogatorie, il richiedente deve presentare anche il modulo e la documentazione aggiuntiva richiesti per il suo caso di deroga (v. n. 5.2.3.5);

3. invitarlo a preparare un PIN con rimando alle pertinenti regole (v. n. 3.16);
4. invito a preparare una passphrase di revoca;
5. indicare i dati di contatto del LRA-Officer per eventuali domande o per convenire una data alternativa.

Per i nuovi collaboratori l'appuntamento può essere fissato anche dal servizio RU competente. Al richiedente dovranno in ogni caso essere inviate le informazioni di cui sopra.

#### 5.2.3.4 Avvio della procedura di rilascio

Il LRA-Officer avvia il walk-in wizard sulla postazione LRA e seleziona la policy corretta (per i certificati di funzione di account di amministratore deve essere selezionata la policy per il rilascio di un singolo certificato di autenticazione). Dopodiché cerca l'utente utilizzando il nome o l'indirizzo e-mail in Admin-Directory e seleziona la registrazione corretta. In questo caso Admin-Directory è la fonte dei dati.

#### 5.2.3.5 Verifica dell'identità del richiedente

Per la verifica dell'identità, il richiedente deve presentarsi personalmente dal LRA-Officer. L'identità del richiedente deve essere verificata sulla base di un passaporto valido o di una carta d'identità riconosciuta per l'entrata in Svizzera. La carta di legittimazione non basta per l'identificazione. La verifica comprende i tre elementi specificati di seguito.

1. La verifica dell'autenticità del documento di viaggio presentato (passaporto o carta d'identità). La carta di legittimazione o la licenza di condurre, ad esempio, non basta per l'identificazione. Devono essere verificati i seguenti elementi:
    a. la validità del documento di viaggio: non deve risultare scaduto al momento della registrazione;
    b. la presenza delle caratteristiche di sicurezza note: devono essere verificate almeno quattro caratteristiche di sicurezza ufficiali del documento;
    c. la corrispondenza tra i dati indicati nel documento e quelli indicati nella richiesta;
    d. la corrispondenza tra la firma apposta nel documento di viaggio e quella apposta nel modulo di richiesta.

2. L'identificazione personale del richiedente mediante il confronto tra la persona e la sua foto riportata nel documento d'identità. Devono essere verificati i seguenti elementi:
    a. la corrispondenza tra la foto sul documento di viaggio e la persona;
    b. la corrispondenza tra l'età e l'altezza riportati sul documento e la persona.

3. La corrispondenza tra i dati del documento nonché della richiesta e i dati registrati in Admin-Directory. In particolare, la corrispondenza del cognome e del nome riportati nel documento con quelli indicati in Admin-Directory deve essere appurata secondo i criteri sottostanti.

    Dal 1° gennaio 2014, per i nuovi collaboratori dell'Amministrazione federale i servizi RU competenti compilano, oltre ai campi «Cognome» e «Nome», anche i campi «Cognome secondo documento» e «Nome secondo documento». Il contenuto di questi campi è visualizzato nella procedura walk-in-wizard. A seconda del contenuto dei quattro campi menzionati sopra, la verifica deve tenere conto delle regole indicate di seguito. La regola applicata deve essere selezionata, apponendo una crocetta, sulla corrispondente schermata del walk-in wizard.

    - **Regola 1:** i due campi «Cognome secondo documento» e «Nome secondo documento» sono compilati e sono identici al cognome/ai cognomi e al nome/ai nomi riportati sul documento di viaggio presentato. Sullo schermo bisogna spuntare l'opzione «Identificato con <Cognome secondo documento> / <Nome secondo documento> come da documento».

    - **Regola 2:** i campi «Cognome secondo documento» e «Nome secondo documento» sono compilati, ma **non** sono identici a quelli riportati sul documento di viaggio presentato. Sullo schermo bisogna spuntare l'opzione «Campo <Cognome secondo documento> / <Nome secondo

documento> non valido».

- **Regola 3:** i campi «Cognome secondo documento» e «Nome secondo documento» non sono compilati, ma il cognome e il nome corrispondono a quelli riportati sul documento di viaggio presentato in considerazione delle condizioni contenute nel documento «Verifica dell'identità dei richiedenti di certificati di classe B» [4]. Sullo schermo bisogna spuntare l'opzione «Identificato con <Cognome> / <Nome>».

- **Regola 4:** i campi «Cognome secondo documento» e «Nome secondo documento» non sono compilati. I campi «Cognome» e «Nome» non corrispondono ai dati riportati sul documento di viaggio, anche in considerazione delle condizioni contenute nel documento «Verifica dell'identità dei richiedenti di certificati di classe B» [4], però sono plausibili. Il richiedente era già in possesso di un certificato con questo nome/i e cognome/i, quindi anche all'atto della sostituzione della scheda o del rilascio di una nuova. È quindi necessario incaricare il servizio RU competente di registrare i dati del richiedente nei campi «Cognome secondo documento» e «Nome secondo documento». Il certificato può essere rilasciato, ma il richiedente deve essere inserito in un elenco dove figurano i certificati rilasciati provvisoriamente. Sullo schermo bisogna spuntare l'opzione «Rilascio provvisorio per <Cognome> / <Nome>». Il LRA-Officer è tenuto a tracciare la procedura di mutazione effettuata dal servizio RU competente nel sistema SIGDP (ex BV Plus).

- **Regola 5:** i campi «Cognome secondo documento» e «Nome secondo documento» non sono compilati e non corrispondono ai dati riportati sul documento di viaggio, anche in considerazione delle condizioni contenute nel documento «Verifica dell'identità dei richiedenti di certificati di classe B» [4]. Al richiedente non è mai stato rilasciato un certificato prima.
  Il certificato non può essere rilasciato. È quindi necessario incaricare il servizio RU competente di registrare i dati del richiedente nei campi «Cognome secondo documento» e «Nome secondo documento». Sullo schermo bisogna spuntare l'opzione «Campo <Cognome> / <Nome> non valido».

***Deroga relativa al permesso F***

In casi eccezionali, l'identificazione può avvenire anche sulla base di un permesso F valido. La procedura di verifica di questo documento deve seguire le stesse regole sopra descritte per i documenti di viaggio. Nelle richieste presentate con permessi F, oltre al modulo di richiesta devono essere presentati anche il modulo e la documentazione aggiuntiva indicati di seguito.

- Il documento «Modulo di richiesta complementare per i richiedenti con permesso F» [5], compilato in tutte le sue parti e firmato dall'ISIU. In questo modulo l'ISIU conferma di non avere potuto identificare chiaramente il richiedente sulla base dei documenti d'identità presentati e accetta il relativo rischio per la propria organizzazione.
- Il permesso di esercitare un'attività lucrativa rilasciato dalle competenti autorità cantonali o federali.

#### 5.2.3.6 Preconfigurazione della scheda

Per motivi di natura strategica, l'Amministrazione federale ha scelto di utilizzare le prestaged smart card. Queste smart card sono preconfigurate centralmente per essere utilizzate dalla SG-PKI e non devono quindi essere inizializzate separatamente. Le non-prestaged smart card non formattate che utilizzano il sistema di gestione dei PUK della SG-PKI sono inizializzate durante la procedura di rilascio con la funzione walk-in wizard o register smart card wizard.

Se viene utilizzato il sistema di gestione dei PUK di altri produttori (ad es. Privacy PUK o Scamiad), bisogna attenersi alle disposizioni interne dell'unità organizzativa e inizializzare prima la smart card con il prodotto terzo osservando le regole di cui al n. 3.18 delle presenti direttive.

#### 5.2.3.7 Digitalizzazione dei documenti

I documenti utilizzati per l'identificazione, in particolare i documenti d'identità, devono essere digitalizzati durante la procedura di rilascio e salvati nel sistema (server in background). Per fare ciò, nella funzione walk-in wizard è a disposizione una procedura di scansione integrata.

Per ottenere risultati di qualità, utilizzare le impostazioni indicate di seguito.

**Colori:** **TrueColor**
**Risoluzione:** **200 x 200** o 300 x 300 (a seconda delle possibilità di impostazione dello scanner)
**Formato:** **JPEG** (estensione file: .jpg)
**PDF** (estensione file: .pdf) per la scansione fronte-retro di entrambi i lati del documento d'identità

Generalmente la procedura di scansione genera un documento A4. Prima di salvare la scansione, ritagliare il documento di viaggio in modo da conservare solo il documento vero e proprio.
Salvare il documento in una cartella personale nel proprio client. Dopo il rilascio del certificato è necessario eliminare questi file ed eventuali e-mail, nonché svuotare il cestino del client e in outlook.

**Importante:** devono essere scansionati **entrambi i lati** dei documenti d'identità, perché la data di scadenza è stampata solo sul retro.

#### 5.2.3.8 Informazioni da trasmettere al richiedente sul PIN e sulla passphrase di revoca

È necessario informare di nuovo il richiedente su senso e scopo della passphrase di revoca. Se non l'ha ancora definita, invitare il richiedente a trovare una frase che sia conforme alle disposizioni di cui al numero 3.17. Inoltre occorre rammentargli le regole per la creazione del PIN secondo quanto spiegato al numero 3.18.

#### 5.2.3.9 Richiesta di certificati e memorizzazione sulla scheda

La smart card del richiedente viene inserita nel secondo lettore. I certificati standard non possono essere caricati sulla stessa scheda in cui sono presenti certificati di classe A o i certificati di funzione di classe B. Per contro, sulla stessa scheda possono essere salvati più certificati di funzione di classe B (ad es. un certificato di amministratore e più certificati di test).

Si passa quindi alla scansione dei documenti richiesti e precedentemente digitalizzati nel sistema (almeno la copia di un documento di viaggio valido). Tutti i documenti necessari per l'identificazione univoca e per la registrazione (ad es. certificato di matrimonio, lettera di fideiussione, altri documenti ecc.) devono essere inseriti in un unico file. La relativa procedura è descritta al n. 5.2.3.7.

Infine il wizard crea la richiesta e la invia al sistema centrale, dove vengono rilasciati i certificati.

L'utente è invitato a inserire il PIN personale e la passphrase di revoca. Dopodiché i certificati sono caricati sulla sua smart card e la scheda è protetta con il PIN personale.

#### 5.2.3.10 Conferma di ricezione dei certificati e firma delle condizioni contrattuali e di utilizzo

Al termine della procedura di rilascio del certificato, stampare un foglio con le impronte digitali del richiedente (caratteristica distintiva inequivocabile di un certificato). Resta ancora da ricordare verbalmente al richiedente quali sono i suoi diritti e obblighi sulla scorta dei documenti «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] e «Linee guida della SG-PKI per i certificati di classe B» [3] (scopo e revoca dei certificati, contenuto della smart card, obbligo di diligenza nella gestione del PIN, passphrase di revoca).

Infine, il richiedente deve firmare una copia delle «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2]. In tal modo attesta di aver letto le informazioni, di averne preso debita nota e di aver ricevuto la smart card con i certificati. Il LRA-Officer confronta la firma apposta su questo modulo con quella apposta sul modulo di richiesta. La copia delle impronte digitali viene allegata alla copia firmata delle condizioni contrattuali. In alternativa, il LRA-Officer può inviare al richiedente le condizioni contrattuali per posta elettronica. In tal caso, il LRA-Officer deve però esigere dal richiedente il rinvio della versione firmata del documento con il certificato di

classe B entro 5 giorni lavorativi e salvare questa versione secondo le direttive sui termini di conservazione di cui al n. 3.8. Se non riceve il documento entro il termine suddetto, il LRA-Officer revoca il certificato.

#### 5.2.3.11 Conclusione della procedura di rilascio

A conclusione della procedura di rilascio il richiedente riceve:

- la nuova smart card;
- le copie non firmate dei documenti «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] e «Linee guida della SG-PKI per i certificati di classe B» [3];
- i suoi documenti di viaggio ed eventualmente gli altri documenti utilizzati.

#### 5.2.3.12 Tenuta del registro

Il LRA-Officer deve annotare le attività svolte nel «Registro della Swiss Government PKI per certificati di classe B» attenendosi alle indicazioni di cui al numero 3.7.

#### 5.2.3.13 Eliminazione dei dati salvati localmente

Se per la scansione di documenti di viaggio non è stata utilizzata la funzione walk-in wizard e i documenti scansionati sono stati salvati localmente, questi devono essere eliminati a rilascio avvenuto. Bisogna inoltre controllare che non sia stato salvato nulla sull'account di posta elettronica personale o aziendale (v. anche n. 5.2.3.7).

Osservazione: è imperativo effettuare l'operazione citata in precedenza, altrimenti si tratterebbe di una collezione di dati non notificata ai sensi della LPD. Va però detto che, durante la procedura di rilascio, i file sono archiviati nella banca dati della SG-PKI, notificata secondo la LPD [29].

#### 5.2.3.14 Archiviazione nel dossier del cliente

La richiesta evasa, la copia firmata del modulo e le «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] vengono archiviate nel dossier del cliente.

Se il dossier del cliente è tenuto in formato elettronico, prima dell'archiviazione occorre scansionare i suddetti documenti, salvarli in formato PDF/A e firmarli dal LRA-Officer con il suo certificato di classe B personale, in modo tale che:

- sia riconoscibile una cronologia;
- sia sempre rintracciabile l'incarico;
- siano disponibili eventuali informazioni in merito a sistemi periferici (ad es. numero del ticket). I ticket pertinenti devono essere reperibili per un periodo di almeno 11 anni dalla scadenza del certificato.

### 5.2.4 Rilascio con RIO

In questo tipo di procedura, denominata anche «procedura di rilascio asincrona», il LRA-Officer delega al RIO l'identificazione del richiedente e altri compiti. Il richiedente e il RIO si trovano in un luogo distante da quello in cui si trova il LRA-Officer. Non è consentito ricorrere a questa procedura per il rilascio di certificati di funzione per account di amministratore.

Per la procedura di rilascio con RIO bisogna inoltre attenersi a questi documenti: «Direttive per il Registration Identification Officer (RIO)» [13] e die «Quickguide WALK-IN ASYNKRON» [14]. In caso di indicazioni contraddittorie si applicano le presenti direttive.

Per ragioni di completezza, in questa sede viene descritta l'intera procedura, quindi anche le operazioni che il richiedente esegue alla fine per attivare la smart card.

#### 5.2.4.1 Compilazione della richiesta

Il richiedente compila la sezione 1 del «Modulo di richiesta per il rilascio di certificati di classe B tramite RIO» con i suoi dati personali, i dati della sua unità organizzativa e i dati per contattarlo. Completa la sezione apponendo data e firma.

#### 5.2.4.2 Identificazione del richiedente da parte del RIO

Il RIO deve accertarsi in maniera inequivocabile dell'identità del richiedente. Perché questo possa avvenire, il richiedente deve recarsi di persona dal RIO. Per eseguire i necessari controlli e integrare il modulo di richiesta con le ulteriori informazioni richieste, è necessario procedere come segue.

1. Il richiedente si reca personalmente da un RIO portando con sé un documento che ne permetta l'identificazione (passaporto o carta d'identità valido).
2. Il RIO procede seguendo la relativa lista di controllo e la compila.
3. Il RIO verifica la corrispondenza tra la foto riportata sul documento di viaggio e il viso del richiedente. Se non vi è corrispondenza, il RIO interrompe la procedura di identificazione e segnala l'irregolarità al LRA-Officer competente. I metodi di identificazione alternativi sulla base di disposizioni derogatorie e le procedure da applicare sono descritti al numero 5.2.3.5. Le disposizioni ivi riportate sono esaustive.
4. Se vi è corrispondenza, il RIO consegna al richiedente una nuova smart card registrata e annota il numero di serie del criptochip nel campo corrispondente del modulo. Se non risulta stampato sulla smart card, il numero di serie può essere richiesto tramite il middleware della scheda o con il wizard di sblocco (unseal wizard). Il RIO fa presente all'utente che da quel momento in poi è lui a essere il solo responsabile della smart card.
5. Apponendo la loro firma in calce alla sezione 2 del modulo di richiesta, il RIO e il richiedente confermano di essersi incontrati di persona, che il RIO ha proceduto all'identificazione del richiedente sulla base di un documento di viaggio valido e che quest'ultimo ha effettivamente ricevuto la smart card di cui sono specificati i dati.
6. Il RIO si accerta che il richiedente abbia letto e compreso le «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] e ne abbia ricevuta una copia. Una seconda copia deve essere firmata dal richiedente.
7. Il RIO posiziona il modulo di richiesta e il documento di viaggio sulla fotocopiatrice in modo che quest'ultimo, con la fotografia del richiedente ben visibile, venga fotocopiato sulla copia della conferma di richiesta nell'apposito campo.
   Devono essere fotocopiati entrambi i lati dei documenti d'identità.
8. Il RIO fotocopia il modulo di richiesta, il documento di viaggio e i moduli e i documenti aggiuntivi richiesti per il rilascio. Il richiedente e il RIO firmano la copia del modulo di richiesta, ora integralmente compilato. Il modulo di richiesta senza il documento di viaggio fotocopiato può essere distrutto.
9. Il RIO invia i due documenti firmati (modulo di richiesta e «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2]), le copie di eventuali documenti aggiuntivi e la lista di controllo compilata al LRA-Officer competente. L'invio può avvenire secondo una delle due modalità seguenti:
   a. i documenti firmati vengono inviati al LRA-Officer competente per posta o corriere,
   b. il RIO scansiona i documenti in formato PDF/A e li firma con il suo certificato standard di classe B valido. Invia poi i documenti così preparati al LRA-Officer competente con un'e-mail crittografata. Il RIO può procedere in questo modo a condizione:
      i. di essere in possesso di un certificato standard di classe B valido;
      ii. di avere accesso alla chiave di crittografia pubblica del LRA-Officer;
      iii. che dalla sua postazione di lavoro sia possibile effettuare scansioni.
10. Se i documenti sono inviati per posta elettronica e il dossier del cliente non viene tenuto in formato elettronico come specificato al numero 5.2.4.3, le relative copie cartacee devono successivamente essere inviate al LRA-Officer per posta ordinaria in modo da poter essere archiviate nel dossier fisico del cliente.

#### 5.2.4.3 Approvazione della richiesta da parte del LRA-Officer

Dopo aver ricevuto e verificato i documenti come descritto al numero 5.2.4.2, il LRA-Officer può approvare la richiesta e autorizzare il rilascio dei certificati. Per farlo esegue le operazioni seguenti indicate nella «Lista di controllo RIO».

1. Il LRA-Officer verifica che siano stati allegati tutti i documenti richiesti e che il modulo di richiesta sia stato firmato da un RIO autorizzato. I documenti richiesti sono:
   - il modulo di richiesta debitamente firmato;
   - le «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] debitamente firmate;
   - la «Lista di controllo RIO» debitamente firmata;
   - altri moduli e documenti richiesti nei casi di deroga.

   Se sono stati trasmessi per e-mail, il LRA-Officer verifica che:
   - i documenti siano stati trasmessi in forma crittografata;
   - i documenti siano stati firmati elettronicamente dal RIO e che la sua firma sia valida.
2. Con la sua smart card, il LRA-Officer avvia la funzione walk-in wizard in modalità RIO sul client LRA. Cerca il richiedente nel sistema, inserendo il suo nome o il suo indirizzo e-mail.
3. Se i moduli sono stati trasmessi in formato cartaceo, il LRA-Officer scansiona le copie del modulo di richiesta e la «Lista di controllo RIO» debitamente firmate ricevute dal RIO, nonché altri moduli e documenti richiesti nei casi di deroga. Per ottenere risultati di qualità, utilizzare le impostazioni indicate di seguito:

   **Colori:** TrueColor
   **Risoluzione:** 200 x 200 o 300 x 300 (a seconda delle possibilità di impostazione dello scanner)
   **Formato:** JPEG (estensione file: .jpg) o PDF/A (estensione file .pdf)

   I documenti ricevuti per via elettronica possono essere inseriti direttamente. Il LRA-Officer carica poi i documenti scansionati con il walk-in wizard.
4. Il LRA-Officer verifica che i dati riportati sul modulo di richiesta corrispondano a quelli riportati sulla copia del documento d'identità e ai dati registrati in Admin-Directory (v. direttive del punto 3 n. 5.2.3.5).
5. Se tutti i dati corrispondono, il LRA-Officer inserisce il numero di serie della smart card consegnata all'utente e approva la richiesta.
6. La richiesta così approvata viene allegata a un ticket e trasmessa alla CA per il rilascio del certificato. Il numero del ticket viene registrato in un documento di sblocco (unseal document) in formato PDF.
7. Il LRA-Officer inoltra il documento o il codice di sblocco (numero del ticket elettronico) direttamente all'utente o al RIO.
8. Il LRA-Officer documenta la procedura nel registro.
9. Il LRO-Officer archivia le «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] firmate nel dossier del cliente.

   Se il dossier del cliente è in formato elettronico, si archivia la versione elettronica firmata dal RIO o il LRA-Officer crea una versione PDF/A dei documenti cartacei e, prima di archiviarla nel dossier, la firma con il suo certificato di classe B. Dal punto di vista della sicurezza di conservazione, della protezione dei dati, della durata di conservazione e dell'idoneità alla revisione, i dossier elettronici dei clienti devono soddisfare i requisiti descritti al n. 5.2.3.13 delle presenti direttive.

#### 5.2.4.4 Installazione del certificato sulla smart card del richiedente

L'ultima cosa da fare è installare il certificato sulla smart card del richiedente. Al proposito, procedere come segue.

1. Dopo il rilascio del certificato il richiedente riceve, per e-mail o tramite RIO, il documento di sblocco con il

numero del ticket elettronico.

2. Il richiedente avvia il wizard di sblocco in un client collegato in rete e inserisce la sua smart card nell'apposito lettore. Se per accedere al client è necessario effettuare il login a due fattori per Windows, bisogna che ci sia un secondo lettore installato. L'utente inserisce il numero di ticket che ha ricevuto. Il wizard verifica che la smart card specificata nel ticket corrisponda a quella inserita nel secondo lettore.
3. Se i dati corrispondono, l'utente è invitato a inserire il PIN personale e la passphrase di revoca.
4. Il wizard memorizza infine la passphrase nella banca dati centrale, carica i certificati sulla smart card e la protegge con il nuovo codice PIN personale.

## 5.3 Procedura di revoca di certificati

### 5.3.1 Persone e organi autorizzati a chiedere una revoca

Le persone e gli organi indicati di seguito sono autorizzati a chiedere la revoca di un certificato (elenco esaustivo):

- il titolare del certificato;
- i collaboratori del servizio RU competente (servizio del personale);
- il superiore diretto;
- il responsabile della SG-PKI;
- il Security Officer PKI;
- il LRA-Officer competente;
- l'ISIU.

### 5.3.2 Modalità di richiesta di una revoca

Il titolare del certificato può richiederne la revoca recandosi di persona dal LRA-Officer, inviandogli un'e-mail o contattandolo per telefono. Il LRA-Officer verifica la plausibilità della richiesta (ad es. con la passphrase di revoca).

I servizi RU o i superiori gerarchici possono inviare le richieste di revoca al LRA-Officer anche sotto forma di elenchi (ad es. file Excel), come si fa soprattutto in caso di uscite o sostituzioni di collaboratori. Il LRA-Officer verifica la competenza del richiedente. Il LRA-Officer può accettare soltanto richieste di revoca inviate per iscritto (e-mail o richieste di revoca firmate). La richiesta di revoca per telefono è riservata esclusivamente ai titolari di un certificato.

Il LRA-Officer, il security officer della SG-PKI e il responsabile della SG-PKI possono revocare un certificato direttamente nell'applicazione della LRA.

### 5.3.3 Motivi di revoca

I motivi principali che portano a una revoca sono i seguenti:

- la smart card è stata rubata o è andata persa;
- la smart card è difettosa;
- la smart card è oggetto di rinnovo;
- il cliente ha dimenticato il PIN della smart card e non esiste un sistema di gestione dei PUK in grado di ripristinare il PIN;
- la smart card è stata bloccata a seguito di troppi tentativi errati di inserimento del PIN e non esiste un sistema di gestione dei PUK in grado di sbloccare la scheda;
- il rapporto di lavoro con il titolare del certificato è cessato;
- i dati contenuti nel certificato sono cambiati (nome, indirizzo e-mail ecc.);
- vi è il sospetto che la chiave privata sia compromessa perché altre persone ne sono venute a conoscenza e hanno utilizzato un servizio (ad es. hanno firmato digitalmente un'e-mail);

- il cliente non rispetta le direttive (ad es. del CP/CPS);
- il LRA-Officer ritiene opportuna una revoca per altri motivi.

#### 5.3.4 Procedura

Una richiesta di revoca deve **sempre essere elaborata immediatamente**. In caso di dubbi circa la validità di una richiesta di revoca (ad es. se è stata fatta per telefono) è bene ricordarsi che lo scopo per cui viene revocato un certificato è di tutelare il cliente da possibili danni derivanti dall'abuso dei suoi certificati. Tuttavia, anche dar seguito a una richiesta di revoca fraudolenta può arrecare danni al cliente, che non può più utilizzare i servizi cui ha diritto. Pertanto, il LRA-Officer deve valutare i danni che potrebbe arrecare una mancata revoca e quelli di una revoca fraudolenta.

Il LRA-Officer procede come descritto di seguito.

##### 5.3.4.1 Verifica della plausibilità della richiesta

Devono essere considerati gli aspetti sottoelencati.

- Il richiedente può essere identificato (voce, numero di telefono, passphrase di revoca)?
- Il servizio RU o il superiore gerarchico è competente per il titolare del certificato in questione?

##### 5.3.4.2 Modulo di revoca

Se viene presentata da terzi, ossia né dal LRA-Officer né dal titolare del certificato (v. n. 5.3.1), la richiesta di revoca deve essere effettuata per iscritto mediante l'apposito «Modulo di revoca per certificati di classe B». Se la richiesta non viene presentata in formato cartaceo, bisogna controllare che il documento o l'e-mail corredata di allegati rechi la firma del richiedente.

Parimenti, è necessario un modulo di revoca se le informazioni (motivo, committente) sulla revoca non sono inserite nel wizard di revoca o se non possono essere revocate mediante il wizard di revoca ufficiale. In questo caso il modulo può essere compilato anche dal LRA-Officer. Questo vale in particolare per revoche mediante la console CMC e per mandati relativi alle revoche indirizzati alla SG-PKI.

##### 5.3.4.3 Revoca

Per procedere alla revoca si avvia il wizard di revoca sulla postazione LRA e si cerca il titolare del certificato. Poi si selezionano i certificati da revocare. Si apre una pagina contenente i documenti d'identità registrati a fronte dello specifico certificato, sulla base dei quali il LRA-Officer può verificare l'identità del titolare del certificato.

Identificato il titolare, si procede alla revoca dei certificati selezionati. Il titolare del certificato riceve automaticamente un'e-mail di conferma dell'avvenuta revoca.

##### 5.3.4.4 Chiusura amministrativa della procedura

Se esiste un modulo di revoca, archiviarlo nel dossier del cliente. Se il dossier del cliente è tenuto elettronicamente, bisogna rispettare le direttive sui termini di conservazione di cui al numero 3.8. La procedura di revoca è documentata nel registro secondo le pertinenti direttive del numero 3.7.

### 5.4 Procedura di rinnovo

I certificati possono essere rinnovati autonomamente dal loro titolare fino a un massimo di due volte prima della loro scadenza (cosiddetta procedura di renewal o rekeying), a condizione che sul client sia installata l'ultima versione del renewal wizard e che la smart card abbia ancora sufficiente spazio di memoria. Poiché nelle prestaged smart card sono già presenti tre serie di chiavi, questa condizione è di norma soddisfatta per questo tipo di scheda. La procedura da seguire è la seguente:

- avviare il renewal wizard sul client della burotica con il certificato di classe B ancora valido;
- viene visualizzata la smart card inserita nel lettore;

- confermare che si tratta della scheda corretta;
- il wizard autorizza quindi la creazione di 3 nuovi certificati e la loro registrazione sulla smart card. I vecchi certificati di firma e di autenticazione vengono eliminati, mentre vengono mantenuti i vecchi certificati di crittografia.

Il rinnovo secondo la procedura sopra descritta non è più possibile dopo la scadenza dei certificati. In questo caso bisogna chiedere al LRA-Officer il rilascio di un nuovo certificato. La procedura è la stessa di quella seguita per il primo rilascio dei certificati.

### 5.5 Procedura di key recovery delle proprie chiavi

Il titolare di un certificato può richiedere direttamente un key recovery per le proprie chiavi di crittografia. La procedura da seguire è la seguente:

con il suo certificato di classe B ancora valido il titolare può collegarsi all'applicazione disponibile alla URL https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/ e aprire un ticket elettronico di key recovery. Con il numero del ticket e la sua smart card si reca poi dal LRA-Officer o dal KRA competente più vicino.

Il LRA-Officer o il KRA identifica l'utente e avvia il key recovery wizard. Inserisce la smart card dell'utente in un lettore libero e inserisce il numero del ticket elettronico. Sullo schermo vengono visualizzate le vecchie chiavi di crittografia dell'utente. Una volta selezionata, la chiave che si vuole recuperare viene aggiunta alle encryption key già presenti sulla smart card.

### 5.6 Procedura di key recovery delle chiavi di terzi

Di principio, le chiavi di crittografia possono essere registrate solo sulla smart card del suo titolare. In casi del tutto eccezionali può essere necessario installare la chiave o le chiavi di crittografia di una persona sulla scheda di un altro utente. I motivi possono essere i seguenti:

- il collaboratore non lavora più per l'unità amministrativa;
- il collaboratore è assente per un lungo periodo a causa di una malattia;
- il collaboratore è deceduto.

Poiché questa procedura consente di leggere tutte le e-mail e tutti i documenti crittografati del titolare del certificato (a condizione che anche i dati crittografati siano in possesso del titolare della chiave), ogni caso deve essere valutato ad hoc. Per questo motivo bisogna inviare al responsabile PKI una richiesta dettagliata e motivata. L'ulteriore modo di procedere è stabilito caso per caso e sempre coinvolgendo il Servizio giuridico.

# 6 Moduli e liste di controllo

Per le procedure descritte in precedenza sono disponibili i moduli e le liste di controllo indicati di seguito, che possono essere ordinati separatamente tramite i responsabili della SG-PKI o sulla pagina Web della SG-PKI.

## 6.1 Modulo di richiesta per il rilascio di un certificato

Prima del rilascio dei certificati con la procedura senza RIO (cfr. n. 5.2.3), il cliente deve compilare il modulo «Modulo di richiesta per il rilascio dei certificati personali di classe B della Swiss Government PKI – Certificati avanzati». Il modulo può essere scaricato dalla pagina web della SG-PKI. I clienti possono predisporne uno ad hoc per la propria organizzazione che comprenda almeno i dati seguenti:

- cognome, nome;
- unità organizzativa;
- indirizzo e-mail;
- numero personale inequivocabile e suffisso.

Il modulo deve inoltre menzionare le regole per la creazione del PIN e della passphrase di revoca personale.

Il modulo deve essere consegnato al cliente in anticipo, in modo che abbia tempo sufficiente per pensare al PIN e alla passphrase di revoca. Il cliente firma il modulo di richiesta e conferma che le informazioni ivi contenute sono corrette.

In alternativa, gli Uffici possono chiedere i certificati di classe B anche avvalendosi del proprio sistema interno di registrazione dei mandati (ad es. Remedy-MAC, GEVER ecc.). In tal caso bisogna fare in modo di attribuire le richieste ai corrispondenti rilasci e conservarle per almeno 11 anni dopo la scadenza della validità del certificato (v. n. 5.2.3.14 e n. 3.8).

Nell'Amministrazione federale il primo rilascio del certificato standard è di norma parte integrante della procedura di entrata di nuovi collaboratori del Servizio RU. Il Servizio RU competente può informare il LRA-Officer dell'arrivo di nuovi collaboratori anche inviandogli un elenco dei nomi, a condizione che su tale elenco siano riportati i dati specificati in precedenza per ciascun nuovo collaboratore.
Per la procedura «Rilascio con RIO» (cfr. n. 5.2.4) si utilizza il « Modulo di richiesta per il rilascio dei certificati di classe B con RIO ».

### 6.1.1 Modulo complementare per richiedenti con il permesso F

Se nel quadro delle disposizioni derogatorie viene presentata una richiesta per un richiedente che ha il permesso F, oltre al normale modulo di richiesta è necessario compilare il «Modulo complementare per richiedenti con il permesso F» debitamente firmato dall'ISIU competente. Apponendo la sua firma, l'ISIU conferma che non è possibile accertare in modo inequivocabile l'identità del richiedente sulla base del permesso F e che, di conseguenza, la SG-PKI non può garantirne la corretta identificazione. Il modulo è parte integrante della documentazione relativa alla procedura di rilascio necessaria ai fini della verifica.

## 6.2 Condizioni contrattuali e di utilizzo per i certificati di classe B

Creato appositamente per l'utente finale, il modulo «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] contiene solo le informazioni più importanti. Le informazioni dettagliate sono riportate nel CP/CPS [1]. Il documento è parte integrante della documentazione relativa alla procedura di rilascio necessaria ai fini della verifica. Il documento «Conferma di ricevuta della smartcard e d'impiego», tuttora disponibile, contiene le impronte digitali dei certificati. Alla fine del documento viene registrato il numero della smart card, se disponibile, che può essere utile in caso di problemi (perdita o danneggiamento della smart card). Il documento è parte integrante della documentazione relativa alla procedura di rilascio necessaria ai fini della verifica.

### 6.3 Modulo di revoca

Nella procedura di revoca con il revoke-wizard, il committente e il motivo di revoca devono essere indicati nel wizard. In questo caso non occorre compilare né archiviare il modulo di revoca. In caso contrario, tale modulo è parte integrante della documentazione relativa alla procedura di rilascio rilevante ai fini delle verifiche. Al proposito si rimanda al n. 5.3.4.2.

### 6.4 Modulo per il recupero di chiavi di terzi

Per questa procedura non esiste un modulo specifico. La richiesta, corredata di motivazione valida, deve essere inviata al responsabile PKI. La documentazione necessaria è parte integrante della documentazione relativa alla procedura di rilascio rilevante ai fini delle verifiche.

### 6.5 Lista di controllo per il rilascio di certificati senza RIO

La «Lista di controllo per il rilascio dei certificati di classe B» serve al LRA-Officer come ausilio per il rilascio dei certificati e non deve essere né compilata né archiviata per ogni certificato rilasciato.

### 6.6 Lista di controllo per il rilascio di certificati con RIO

La «Lista di controllo per il rilascio con RIO» serve al LRA-Officer come ausilio per il rilascio dei certificati e non deve essere né compilata né archiviata per ogni certificato rilasciato.

### 6.7 Lista di controllo RIO

La «Lista di controllo RIO» è un elemento essenziale della richiesta nell'ambito della procedura con RIO. Il RIO deve compilarla per ogni richiesta e inviarla al LRA-Officer incaricato dell'autorizzazione per archiviazione nel dossier del cliente. Questa lista di controllo è parte integrante della documentazione relativa alla procedura di rilascio necessaria ai fini della verifica.

### 6.8 Lista di controllo per la revoca di certificati

La «Lista di controllo per la revoca dei certificati di classe B» serve al LRA-Officer come ausilio per il rilascio dei certificati e non deve essere né compilata né archiviata per ogni certificato revocato.

## 7 Reclami

In caso di domande o problemi con i clienti, la SG-PKI o altre unità organizzative che non possono essere risolti autonomamente, contattare i responsabili PKI dell'UFIT.

## 8 Proposte di modifica

Eventuali osservazioni o proposte di modifica riguardanti il presente documento possono essere inviate al seguente indirizzo:

Responsabile servizio SG-PKI
Ufficio federale dell'informatica e della telecomunicazione
Monbijoustrasse 74
CH-3003 Berna
e-mail: pki-info@bit.admin.ch

# ALLEGATI

## Allegato A: liste di controllo delle procedure per i certificati di classe B

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

## Procedura per il rilascio dei certificati di classe B («Rilascio senza RIO», n. 5.2.3 delle direttive per la registrazione)

V2.1, 20.09.2019

| N. | Descrizione | Direttiva di riferimento[1] |
|---|---|---|
| ***Lavori preliminari*** | | |
| 1. | Verificare la richiesta: | |
| | a) Il richiedente è registrato in Admin-Directory? Il nome registrato è corretto e comprensivo di suffisso e indirizzo di posta elettronica? | 5.2.3.1 |
| | b) Il richiedente è autorizzato a ottenere un certificato di classe B? Si trova nel ramo dell'Admin-Directory di competenza del LRA-Officer? | 5.2.1 |
| | c) L'indirizzo di posta elettronica indicato nel modulo di richiesta coincide con quello in Admin-Directory? | 5.2.3.2 |
| | d) I dati indicati nel modulo di richiesta sono completi e plausibili? | 5.2.3.2 |
| 2. | Fissare l'appuntamento per il rilascio del certificato inviando un'e-mail all'indirizzo indicato dal richiedente, specificando che gli unici documenti di identificazione accettati sono il passaporto e la carta d'identità. Può essere utile fornire prima dell'appuntamento le informazioni su come scegliere il PIN e la passphrase di revoca. | 5.2.3.3 |
| 3. | Preparare la smart card, che dovrà essere inizializzata separatamente solo se per la gestione dei PUK viene utilizzato un software di terzi. Tutte le altre carte sono già state preparate al momento della preconfigurazione oppure vengono formattate come prima cosa dal walk-in wizard durante la loro preparazione. | 5.2.3.6 |
| ***Rilascio*** | | |
| 4. | Verificare l'identità del richiedente: | 5.2.3.5 |
| | a) Il documento di viaggio è un passaporto o una carta d'identità? Il richiedente può essere identificato sulla base di un altro documento nel quadro delle disposizioni derogatorie? Il documento d'identità è autentico? (Verificare almeno 4 indicatori di sicurezza) | |
| | b) Il documento (di viaggio) è valido? | |

[1] Direttive per la registrazione dei certificati di classe B della Swiss Government PKI.

| | | |
|---|---|---|
| | c) I dati della richiesta corrispondono a quelli del documento (d'identità) nonché ai dati registrati in Admin-Directory, in particolare il cognome e il nome del richiedente? | |
| | d) Confrontare il viso del richiedente con la foto del documento (d'identità). Si tratta della stessa persona? | |
| 5. | Digitalizzare e salvare il documento ed eventuali altri documenti necessari. | 5.2.3.7 |
| 6. | Fornire al richiedente le informazioni necessarie per la scelta del PIN e della passphrase di revoca (queste informazioni possono anche essere fornite con l'e-mail di invito). | 5.2.3.8 |
| 7. | Emettere la smart card mediante il walk-in wizard. Durante questa fase l'utente deve inserire personalmente il PIN e la passphrase di revoca scelti. | 5.2.3.9 |
| 8. | Informare il richiedente sugli obblighi contenuti nelle «Condizioni contrattuali e di utilizzo per i certificati di classe B» e nelle «Linee guida della SG-PKI per i certificati di classe B» e chiarire con lui ogni aspetto della questione. | 5.2.3.10 |
| 9. | Aggraffare il documento «Conferma di ricevuta della smart card e d'impiego» alla documentazione firmata (operazione facoltativa) e far firmare una copia delle «Condizioni contrattuali e di utilizzo per i certificati di classe B» e delle «Linee guida per i certificati di classe B». | 5.2.3.10 |
| 10. | La firma sulle «Condizioni contrattuali e di utilizzo per i certificati di classe B» corrisponde a quella sul documento d'identità? | |
| 11. | Consegnare al richiedente la smart card, il documento di viaggio nonché le copie non firmate delle «Condizioni contrattuali e di utilizzo per i certificati di classe B» e delle «Linee guida della SG-PKI per i certificati di classe B». | 5.2.3.11 |
| 12. | Annotare nel registro le operazioni svolte. | 5.2.3.12 |
| 13. | Eliminare il file creato al punto 5 relativo al documento (d'identità) ed eventuali e-mail di invio. | 5.2.3.13 |
| 14. | Archiviare la copia firmata delle «Condizioni contrattuali e di utilizzo per i certificati di classe B», la richiesta (se presentata in formato cartaceo) e le impronte digitali dei certificati nel dossier del cliente. | 5.2.3.14 |

# Lista di controllo per il rilascio dei certificati di classe B con RIO per LRAO

## Procedura per il rilascio dei certificati di classe B (v. «Rilascio con RIO», n. 5.2.4 delle direttive per la registrazione)

V2.1, 20.09.2019

| Descrizione | Direttiva di riferimento[1] |
|---|---|
| ***Compilazione della richiesta*** | |
| Il richiedente/il collaboratore RU/il superiore gerarchico compila la prima parte del modulo per la richiesta di un certificato mediante RIO e wizard e informa il RIO (e il cliente) della necessità di rilasciare un nuovo certificato (https://www.bit.admin.ch/bit/it/home/subsites/la-swiss-government-pki-in-generale.html). | 5.2.4.1 |
| ***Identificazione del richiedente e inoltro della richiesta da parte del RIO*** | |
| Il RIO procede seguendo la «Lista di controllo RIO», documenta le singole fasi e inoltra i documenti al LRA-Officer. È importante che nel modulo di richiesta venga indicato il numero di serie della smart card e che le copie/scansioni dei documenti siano complete e leggibili. | 5.2.4.2 |
| ***Approvazione del rilascio dei certificati da parte del LRA-Officer*** | |
| Verifica della richiesta: | 5.2.4.3 |
| a) Sono disponibili tutti i documenti necessari (modulo di richiesta con numero di serie della scheda, lista di controllo, copia firmata delle «Condizioni contrattuali e di utilizzo per i certificati di classe B»)?<br>**In caso di trasmissione elettronica**: i documenti sono stati tutti trasmessi in forma crittografata? | |
| b) La conferma della richiesta è stata firmata da un RIO autorizzato?<br>**In caso di trasmissione elettronica**: la firma elettronica del RIO è valida? | |
| c) Scansionare e salvare la copia del documento (d'identità) ed eventuali altri documenti.<br>**In caso di trasmissione elettronica**: salvare la conferma della richiesta firmata. | |
| d) Confrontare i dati presenti nel sistema con quelli riportati sul modulo di richiesta: l'utente è registrato correttamente in Admin-Directory? | |
| Rilascio dei certificati tramite il walk-in wizard: utilizzare il modello RIO. | |
| e) Aggiungere i documenti scansionati. La richiesta così approvata viene allegata a un ticket e trasmessa alla CA per il rilascio del certificato. Il numero del ticket viene registrato in un documento di sblocco (unseal document) in formato pdf. | |
| f) Inviare il documento di sblocco (unseal document) con il codice di attivazione all'indirizzo privato del cliente (in alternativa i dati di attivazione possono essere inviati al RIO con un'e-mail crittografata e firmata). | |

[1] Direttive per la registrazione dei certificati di classe B della Swiss Government PKI.

| | |
|---|---|
| g) Archiviare i documenti di cui al punto a) in formato cartaceo nel dossier del cliente e, in caso di **trasmissione elettronica**, nel dossier elettronico del cliente. | |
| h) Annotare tutte le operazioni nel registro. | 5.2.4.3, 3.7 |
| ***Ritiro del certificato da parte del richiedente*** | |
| 1) Aprire il wizard di sblocco del token (token unseal wizard) presso il RIO o un collega in possesso di un secondo lettore di schede. | |
| 2) Inserire la scheda nel lettore → Viene automaticamente riconosciuta dal sistema. | |
| 3) Se il wizard lo richiede, inserire il codice di attivazione → I certificati vengono registrati. | |
| 4) Inserire il PIN e la passphrase di revoca → La scheda è pronta per l'utilizzo. | |

# Lista di controllo per la revoca dei certificati di classe B

## Procedura per la revoca dei certificati di classe B (v. «Procedura di revoca di certificati», n. 5.3 delle direttive per la registrazione)

V2.1, 20.09.2019

| N. | Descrizione | Direttiva di riferimento[1] |
|---|---|---|
| ***Verificare la richiesta*** | | |
| 1. | Verificare la plausibilità della richiesta. | 5.3.4.1 |
| 2. | Se necessario e non è già stato fatto dal richiedente, compilare il modulo di revoca. | 5.3.4.2 |
| ***Revocare il certificato*** | | |
| 3. | Cercare il relativo certificato nel revoke wizard. | 5.3.4.3 |
| 4. | Identificare il titolare del certificato sulla base dei documenti d'identità salvati. | |
| 5. | Revocare i certificati. | |
| ***Concludere l'operazione di revoca*** | | |
| 6. | Archiviare il modulo di revoca (se possibile, sulla base della procedura o dell'applicazione selezionata). | 5.3.4.4 |
| 7. | Annotare le operazioni nel registro. | 5.3.4.4, 3.7 |

[1] Direttive per la registrazione dei certificati di classe B della Swiss Government PKI.

# Lista di controllo RIO

**V2.1, 20.09.2019**

| N. | Descrizione dei compiti | SÌ/NO | Data |
|---|---|---|---|
| 1 | Verificare la plausibilità della richiesta → Il richiedente è autorizzato a ottenere certificati di classe B della Swiss Government PKI e i suoi dati sono registrati nell'Admin-Directory della Confederazione. | | |
| 2 | Verificare l'identità confrontando un documento di viaggio valido con il modulo di richiesta (accettare solo la carta d'identità valida o il passaporto valido). | | |
| | Cognome: _____ | | |
| | Tipo di documento d'identità in base al modulo di richiesta (solo carta d'identità valida, passaporto valido o caso di deroga spiegato nelle direttive)<br>N. del documento: _____<br>Validità del documento di viaggio: _____ | ☐ Carta d'identità<br>☐ Passaporto<br>☐ Altro | |
| | Confrontare il viso del richiedente con la foto del documento di viaggio. | | |
| 3 | Consegnare la smart card preconfigurata (o prestaged). Informare l'utente che da quel momento in poi è l'unico responsabile della scheda.<br>Numero di serie della smart card: _____ | | |
| 4 | Compilare la parte 2 del modulo di richiesta e firmare. | | |
| 5 | Spiegare al cliente il contenuto delle Condizioni contrattuali e di utilizzo per i certificati di classe B» e le «Linee guida della SG-PKI per i certificati di classe B». | | |
| 6 | Far firmare due copie delle «Condizioni contrattuali e di utilizzo per i certificati di classe B» e delle «Linee guida della SG-PKI per i certificati di classe B» e consegnarne una al cliente. | | |
| 7 | Fotocopiare il documento d'identità sul retro del modulo (carte d'identità: fronte-retro). Fotocopiare tutti i documenti. | | |
| 8 | Firmare tutte le pagine recanti la fotocopia del documento d'identità e farle firmare al cliente. | | |
| 9 | Firmare la presente lista di controllo. | | |
| 10 | Inviare i documenti al LRA-Officer (le «Condizioni contrattuali e di utilizzo per i certificati di classe B», il modulo di richiesta compilato e la presente lista di controllo).<br>In caso di trasmissione elettronica: crittografare i documenti firmati e inviarli per e-mail al LRA-Officer competente. | | |

| Cognome e nome del RIO: | Unità organizzativa: | Luogo e data: |
|---|---|---|

Firma del RIO: _____

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Esercizio
Esercizio servizi front end
PKI

# Allegato B: moduli e direttive per i certificati di classe B

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Esercizio
Esercizio servizi front end
PKI

**NON CLASSIFICATO**

# Modulo di richiesta per il rilascio dei certificati personali di classe B della Swiss Government PKI

## Certificati avanzati

V2.3, 20.09.2019

Il presente modulo serve per richiedere un certificato di classe B della Swiss Government PKI. Si opera una distinzione tra i certificati standard (con autenticazione, firma e crittografia) e i certificati di funzione per account di amministratore e account di test (per i primi solo autenticazione).

**Per l'identificazione presso l'autorità di registrazione occorre una carta d'identità valida o un passaporto valido.**

** Campi obbligatori*

| | |
|---|---|
| Cognome e nome/i*: | |
| N. documento d'identità*: | Valido fino a*: |
| Unità organizzativa*: | |
| Tipo di certificato*: certificato di classe B standard | |
| E-mail*: | |
| Indirizzo aziendale*: | |
| Luogo d'origine: | Data di nascita: |
| N. smart card: | |

**Luogo e data*:** **Firma*:**

_____ _____

**NON CLASSIFICATO**

# Modulo di richiesta complementare per i richiedenti con permesso F

V1.1, 20.09.2019

Il presente modulo è parte integrante della richiesta per l'ottenimento di un certificato di classe B della Swiss Government PKI. Deve essere compilato se il richiedente è sprovvisto di un documento di viaggio valido e se possiede soltanto un permesso F.

**Il presente modulo deve essere inoltrato unitamente al modulo di richiesta per il rilascio di certificati di classe B della Swiss Government PKI compilato in tutte le sue parti e munito di firma valida.**

Il presente modulo deve essere firmato dall'ISIU competente. Apponendo la sua firma, l'ISIU conferma che non è possibile accertare in modo inequivocabile l'identità del richiedente sulla base del permesso F e che, di conseguenza, la SG-PKI non può essere resa responsabile del fatto che la vera identità del richiedente non può essere accertata.

| | |
|---|---|
| Cognome: | Nome: |
| N. del documento d'identità: | |
| Unità organizzativa: | |
| Tipo di certificato:<br>certificato standard ☐<br>certificato di funzione:<br>amministratore ☐<br>test ☐ | |
| E-mail[1]: | |
| Indirizzo aziendale: | |
| Luogo d'origine: | Data di nascita: |
| ☐ Collaboratore interno | ☐ Collaboratore esterno |

[1] Indirizzo e-mail del titolare dell'account se la richiesta riguarda un certificato di funzione per amministratore.

**ISIU**

Cognome e nome: _____
(in stampatello)

Luogo e data: _____

Firma: _____

**Richiedente**

N. di serie del documento: _____

Luogo e data: _____

Firma: _____

# Modulo di richiesta per il rilascio dei certificati di classe B con RIO

## Modulo di trasmissione delle informazioni del richiedente al LRA-Officer

V1.1 20.09.2019

### 1 Dati del richiedente (compilazione a cura del richiedente e consegna al RIO)

Con il presente modulo il richiedente ordina una smart card preconfigurata per il rilascio di certificati di classe B della Swiss Government PKI:

Cognome e nome:

Dipartimento, Cantone o ufficio:

Indirizzo e-mail:

Numero di telefono:

Luogo e data

Firma: _____

### 2 Identificazione e consegna della scheda (compilazione congiunta da parte del RIO e del richiedente, consegna al LRA-Officer)

Il richiedente riceve dal RIO una smart card preconfigurata che, dopo l'approvazione della richiesta da parte del LRA-Officer, può essere sbloccata tramite l'apposito S-PIN che gli è stato consegnato o inviato.

Il RIO assegna al richiedente la smart card
il numero distintivo seguente:

n. di serie (obbligatorio): _____
n. di carta o carta di legittimazione (facoltativo): _____

Apponendo la propria firma il RIO e il richiedente confermano di essersi incontrati personalmente, che la smart card con il summenzionato numero di serie è stata consegnata e che l'identità del richiedente è stata verificata sulla base di un documento di viaggio valido.

**RIO**

Cognome e nome: _____
(in stampatello)

Luogo e data: _____

Firma: _____

**Richiedente**

N. di serie del documento: _____

Luogo e data: _____

Firma: _____

### 3 Condizioni contrattuali e di utilizzo per i certificati di classe B

Il RIO si accerta che il richiedente abbia letto e compreso le «Condizioni contrattuali e di utilizzo per i certificati di classe B» [2] e ne abbia ricevuta una copia. Il richiedente deve firmare una seconda copia, che in seguito il RIO consegna al LRA-Officer unitamente al presente modulo compilato e alle copie dei documenti di viaggio.

**4 Fotocopia del documento di viaggio**

Sul retro del presente modulo deve essere fotocopiato un documento di viaggio valido del richiedente. È imperativo fotocopiare le carte d'identità fronte-retro. Le copie del passaporto devono mostrare le pagine recanti foto, firma e validità. Il retro dei documenti e le ulteriori pagine utilizzate devono essere firmate da entrambe le parti, indicando luogo e data. Utilizzare il retro del presente modulo come supporto per fotocopiare i documenti.

[Posizionare qui i documenti d'identità da fotocopiare]

**RIO**

Luogo e data: _____

Firma: _____

**Richiedente**

Luogo e data: _____

Firma: _____

**NON CLASSIFICATO**

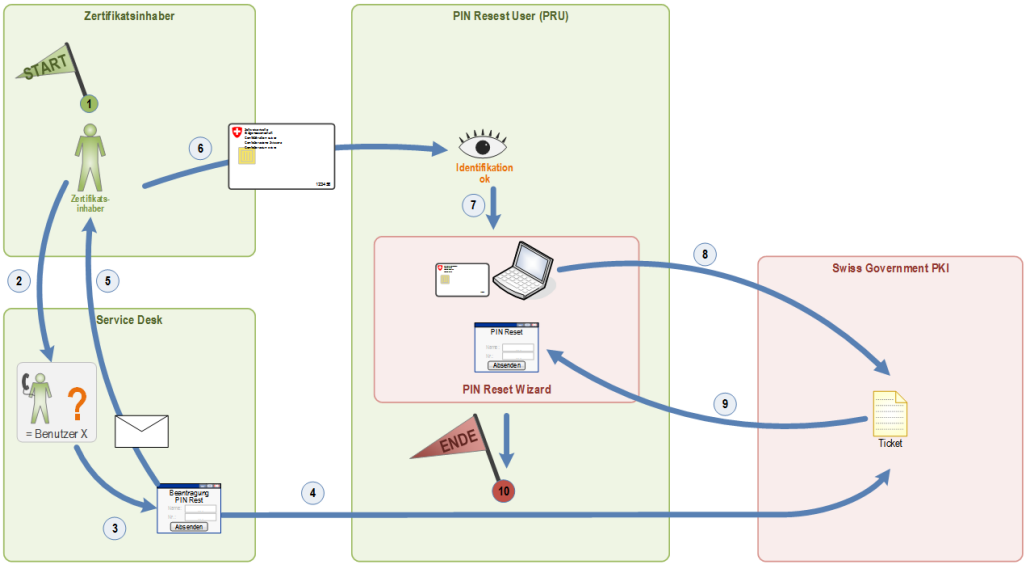
# Modulo di richiesta di reset del PIN per i superuser e i service desk

## Autorizzazione per aprire ticket online

V1.1 25.10.2019

Il presente modulo serve a ottenere l'autorizzazione ad aprire ticket online per il reset del PIN delle smart card e può essere compilato soltanto dai collaboratori del service desk o dai superuser. L'autorizzazione costituisce la prima parte della procedura di reset del PIN delle prestaged smart card. L'utente interessato deve, in un secondo momento, attivare la smart card dal client di un collaboratore e inserire il nuovo PIN per la sua smart card. Al proposito si rimanda anche alla scheda informativa sui PRU disponibile al link:
https://www.bit.admin.ch/bit/it/home/subsites/la-swiss-government-pki-in-generale.html.

**Procedura di reset del PIN**




**Dati del richiedente**

Cognome e nome, suffisso:

Dipartimento o Cantone:

Ufficio:

Funzione:

Indirizzo e-mail:

N. tel.:

N. Serie del certificato d'autenticazione

Data:

*Firma digitale*: _____

**Autorizzazione (con marca temporale)**

*Firma digitale responsabile organizzazione*:

_____

*Firma digitale capo dell'ufficio*:

_____

*Firma digitale security officer SG-PKI*:

_____

**Revoca dell'autorizzazione**

Si prega di revocare l'autorizzazione di aprire ticket online per richieste di reset del PIN della persona suindicata (denominata *richiedente*) ☐

**NON CLASSIFICATO**

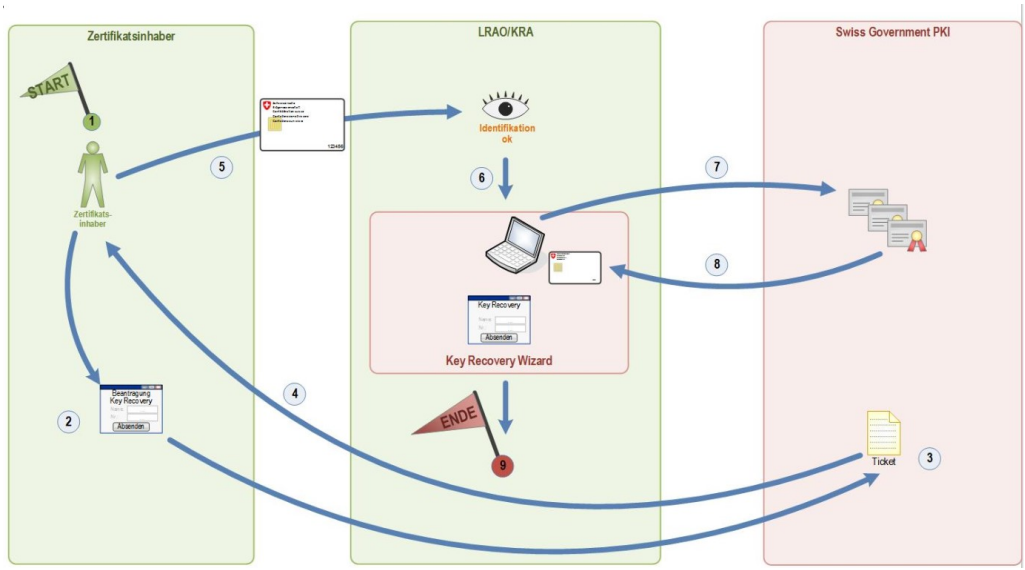
# Modulo di richiesta per il key recovery agent (KRA)

## Autorizzazione per eseguire il key recovery wizard

V1.1 25.10.2019

Il presente modulo serve ad autorizzare un RIO, un collaboratore, un'organizzazione di supporto informatico o un superuser di operare in qualità di key recovery agent (KRA). Tale autorizzazione è necessaria per eseguire la seconda parte del processo di key recovery. L'utente che ne ha bisogno consulta dal proprio browser la pagina web «Key Recovery» (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/ ) e vi elabora un **ticket elettronico** nel sistema centrale PKI. Dopo aver ricevuto il ticket dal titolare dei certificati, il KRA lancia il key recovery wizard e inserisce il numero del ticket elettronico. Il wizard visualizza quindi tutti i certificati di crittografia rilasciati per questo titolare di certificati. Il titolare dei certificati fornisce al KRA la chiave che desidera ripristinare. Dopo l'immissione del PIN personale, il wizard scrive le encryption key desiderate sulla smart card del titolare dei certificati.

**Procedura di key recovery**




**Dati del richiedente**

Cognome e nome e suffisso:

Dipartimento/Cantone:

Ufficio:

Funzione:

Indirizzo e-mail:

N. tel.:

N. Serie del certificato d'autenticazione:

Data:

*Firma digitale*: _____

**Autorizzazione (con marca temporale)**

*Firma digitale responsabile organizzazione*:

_____

*Firma digitale capo dell'ufficio*:

_____

*Firma digitale security officer SG-PKI*:

_____

**Revoca dell'autorizzazione**

Si prega di revocare l'autorizzazione di KRA della persona suindicata (denominata *richiedente*) ☐

**NON CLASSIFICATO**

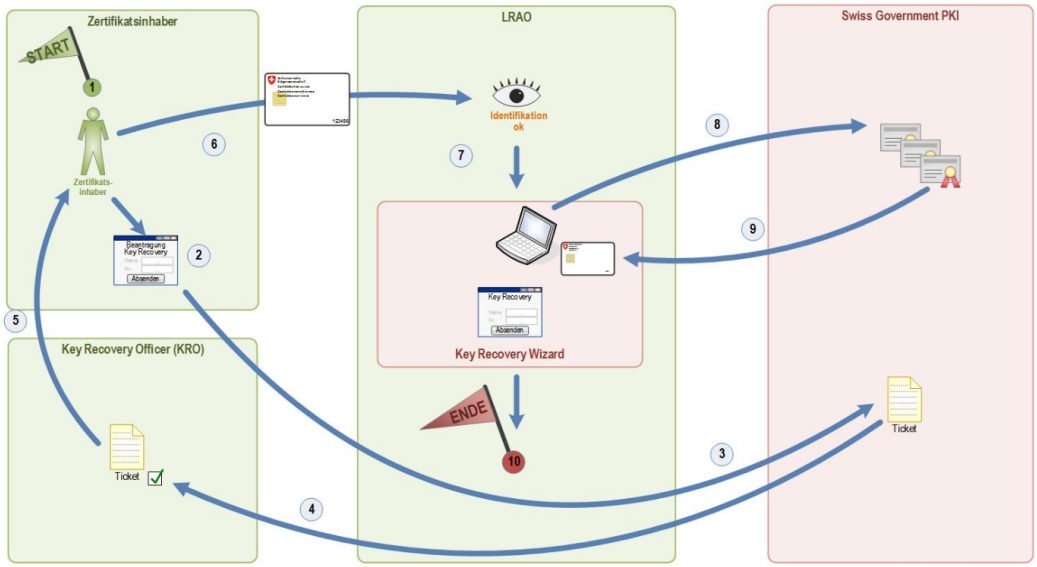
# Modulo di richiesta per il key recovery officer (KRO)

## Autorizzazione per eseguire richieste di key recovery

V1.1 25.10.2019

Il presente modulo serve ad autorizzare un RIO, un collaboratore, un'organizzazione di supporto informatico o un superuser di operare in qualità di key recovery officer (KRO). Tale autorizzazione è necessaria per eseguire la seconda parte del processo di key recovery con KRO. L'utente che ne ha bisogno consulta dal proprio browser la pagina web «Key Recovery» (https://keyrecovery.pki.admin.ch/KeyRecoveryRequest/ ) e vi elabora un **ticket elettronico** nel sistema centrale PKI. In seguito, spetta al KRO verificare la richiesta ed eventualmente approvarla prima che il titolare dei certificati si rechi con il proprio **ticket elettronico** dal LRA-Officer o dal KRO. Il LRA-Officer o il KRA lancia quindi il key recovery wizard e inserisce il numero del **ticket elettronico**. Il wizard visualizza quindi tutti i certificati di crittografia rilasciati per questo titolare di certificati. Il titolare dei certificati indica le chiavi che intende ripristinare. Dopo l'immissione del PIN personale, il wizard scrive le encryption key desiderate sulla smart card del titolare dei certificati.

**Procedura di key recovery con KRO**




**Dati del richiedente**

Cognome e nome e suffisso:

Dipartimento/Cantone:

Ufficio:

Funzione:

Indirizzo e-mail:

N. tel.:

N. Serie del certificato d'autenticazione

Data:

*Firma digitale*: _____

**Autorizzazione (con marca temporale)**

*Firma digitale responsabile organizzazione*:

_____

*Firma digitale capo dell'ufficio*:

_____

*Firma digitale security officer SG-PKI*:

_____

**Revoca dell'autorizzazione**

Si prega di revocare l'autorizzazione di KRO della persona suindicata (denominata *richiedente*) ☐

**NON CLASSIFICATO**

# Modulo di revoca per certificati di classe B
## Swiss Government PKI

V2.4, 20.09.2019

| **Richiedente** | | | |
|---|---|---|---|
| ☐ **Titolare del certificato** | ☐ **Superiore** | ☐ **RU** | ☐ **ISIU** |
| ☐ **Responsabile PKI** | ☐ **LRA-Officer** | ☐ **Security officer della SG-PKI** | |
| Cognome: | | Nome: | |
| Unità organizzativa: | | | |

| **Titolare del certificato**<br>(* compilare solo se il titolare del certificato e il richiedente non sono la stessa persona) | | |
|---|---|---|
| Cognome*: | Nome*: | Suffisso*: |
| Unità organizzativa*: | | |
| Tipo di certificato:<br>☐ certificato standard<br>☐ certificato di funzione per amministratore<br>☐ certificato di funzione per test | | |
| ☐ collaboratore interno<br>☐ collaboratore esterno<br>☐ lista di revoca | | |

| **Motivo della revoca** | |
|---|---|
| ☐ Smart card smarrita | ☐ Smart card difettosa |
| ☐ Sospetta compromissione | ☐ Uscita |
| ☐ Errore nel rilascio | ☐ Sospetto abuso |
| ☐ Altro: | |

| | |
|---|---|
| Certificato revocato in data: | |
| LRA-Officer responsabile della revoca (cognome, nome): | Firma:<br><br>_____ |

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Swiss Government PKI

# Registro del LRA-Officer della Swiss Government PKI per certificati di classe B

V2.1, 20.09.2019

| N. progressivo | Data | Cliente | Attività:<br>CS: certificato standard, CFA: certificato di amministratore, CFT: certificato di test,<br>RI: rilascio, RE: revoca, K: key recovery | N. di serie della smart card | Smart card ritirata<br>SÌ/NO | Visto LRA-Officer |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
**Ufficio federale dell'informatica e della telecomunicazione UFIT**
Swiss Government PKI

**NON CLASSIFICATO**

# Modulo di richiesta per LRA-Officer per certificati di classe B

V4.5, 20.09.2019

☐ **Nuovo LRA-Officer** → Sez. A e B ☐ **Rinnovo LRA-Officer** → Sez. A e B ☐ **Modifica autorizzazioni** → Sez. B ☐ **Revoca del certificato di LRA-Officer** → Sez. C

**Sezione A) – Prima di elaborare la richiesta devono essere soddisfatti i requisiti sottostanti.**

☐ Formazione assolta, test superato: allegare la copia dell'attestato e la conferma del superamento del test.

☐ Nome registrato nelle pagine gialle dell'Admin-Directory.

☐ Informazioni sul LRA-Officer → sezione B compilata in modo corretto ed esaustivo.

**Sezione B) – Dati relativi al LRA-Officer e alle autorizzazioni per il rilascio di certificati**

**Rilascio di certificati di classe B per l'Amministrazione federale:**
☐ l'indirizzo e-mail termina con «admin.ch» (prestaged/enhanced CA02)
☐ l'indirizzo e-mail *non* termina con «admin.ch» (prestaged/enhanced CA01)

**Rilascio di certificati di classe B per persone esterne all'Amministrazione federale:**
☐ prestaged enhanced CA01)
☐ *non*-prestaged/standard (enhanced CA01)

| **Dati sul LRA-Officer (devono corrispondere ai dati inseriti in Admin-Directory) (* campi obbligatori)** | | | |
|---|---|---|---|
| Cognome*: | | Nome*: | |
| Suffisso*: | | Dipartimento*: | |
| Ufficio*: | | Tel.*: | |
| E-mail*: | | | |
| Indirizzo (via, NPA, luogo)*: | | | |
| Autorizzazione per il rilascio di certificati per (dipartimento, ufficio)*: | | ☐ nuovo ☐ revocato | |
| N. di serie certificato personale di classe B di autentificazione | | | |
| Autorizzazione per i certificati di **account di amministratore** (A-account) a livello dipartimentale | ☐ nuovo ☐ revocato per il dipartimento: DFF | | |

**Sezione C) – Prima di trattare la richiesta devono essere soddisfatti i requisiti sottostanti.**

Data di esecuzione della revoca:

C'è un LRA-Officer subentrante? ☐ No ☐ Sì, nome e cognome:

☐ Informazioni sul LRA-Officer → **Sezione B** compilata in modo corretto ed esaustivo.

Il LRA-Office ancora in servizio si impegna a consegnare alla persona subentrante il dossier cliente e il registro. Inoltre, il LRA-Officer uscente è tenuto a restituire la propria smart card.

**Condizioni generali di utilizzo per il LRA-Officer**

**Dichiarazione di confidenzialità**

*Con la sua firma, il richiedente si impegna ad utilizzare la smart card e la relativa password garantendone la riservatezza e a non divulgare le informazioni personali trattate nell'ambito della sua attività a terzi, ma solo ai collaboratori interni che devono poter accedere direttamente a tali informazioni per svolgere i loro compiti. I collaboratori che svolgono la funzione di LRA-*

*Officer sono tenuti alla tutela del segreto professionale, se non è già stato stabilito nel contratto di lavoro. Non è consentito fotocopiare né integralmente né parzialmente i dati e le informazioni da elaborare.*

*Il LRA-Officer è obbligato a far revocare il certificato in caso di cessazione della sua funzione. La presente dichiarazione è valida anche dopo la cessazione della funzione di LRA-Officer e dopo la sua uscita dall'organizzazione.*

*Ai certificati per LRA-Officer si applicano le disposizioni contenute nelle «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI», nelle «Linee guida per l'ottenimento del certificato di LRA-Officer della Swiss Government PKI» (v. pagine seguenti) e nelle «Direttive per la registrazione dei certificati di classe B della Swiss Government PKI». Secondo i CP/CPS in vigore, firmando i documenti, l'aspirante LRA-Officer della SG-Root CA I dichiara di aver letto, compreso e accettato tutte le disposizioni e le procedure ivi descritte e di rispettarle integralmente. Con la sua firma, l'aspirante LRA-Officer accetta altresì che gli venga rilasciata una smart card personale per espletare la funzione di LRA-Officer.*

| **Richiedente (nome, cognome)** | **Data** **Firma** |
|---|---|
| | |

**Verifica dell'affidabilità**

L'autorità ha preso ogni misura ragionevolmente esigibile e permessa dalla legge per accertare l'affidabilità e l'integrità del candidato. La SG-PKI raccomanda all'autorità di adottare le seguenti misure:

- controllo di sicurezza di base secondo l'articolo 10 OCSP presso il servizio specializzato CSP DDPS;
  *e/o*
- adottare misure proprie per verificare l'affidabilità del candidato, ad esempio:
  - il controllo dell'identità del candidato (passaporto o carta d'identità),
  - la verifica delle referenze professionali e private del candidato,
  - la verifica della completezza e coerenza del curriculum vitae del candidato,
  - il controllo delle qualifiche accademiche e professionali dichiarate,
  - la verifica degli estratti dal registro delle esecuzioni e dal casellario giudiziale.

**Conferma**

Il collaboratore dell'autorità avente diritto di firma conferma alla SG-PKI l'affidabilità del candidato conformemente alla summenzionata raccomandazione o di aver effettuato la verifica in modo analogo. Il collaboratore considera il candidato sia affidabile e integro nonché che possieda le competenze necessarie per la funzione di LRA-Officer, sensibile sotto il profilo della sicurezza.

**Firme**

Se l'iter burocratico di autorizzazione coinvolge diversi uffici, è necessaria la firma di ognuno dei responsabili aventi diritto di firma. Al proposito si prega di utilizzare anche l'elenco di moduli disponibile sul sito www.pki.admin.ch.

Le persone aventi diritto di firma sono:

- a **livello di ufficio federale**: gli ISIU, i responsabili PKI dei Cantoni/del corpo di polizia, gli incaricati della sicurezza degli uffici cantonali, il consiglio di amministrazione del SG-PKI;
- a **livello di dipartimento**: gli ISID, i responsabili delle PKI dei Cantoni/della polizia cantonale, gli incaricati della sicurezza degli uffici cantonali/della polizia cantonale.

| **Ufficio della persona avente diritto di firma (nome, cognome, funzione)** | **Data** **Firma** |
|---|---|
| | |

Per l'attribuzione dei diritti per i singoli account di amministratore (solo interni all'Amministrazione federale) è necessaria la firma dell'**ISID** (*l'autorizzazione è valida sempre per tutto il dipartimento*). Se l'iter burocratico di autorizzazione coinvolge diversi dipartimenti, gli ISID di tutti i dipartimenti interessati devono apporre la loro firma nel campo sottostante. Al proposito si prega di utilizzare anche l'elenco di moduli disponibile sul sito www.pki.admin.ch.

| **Dipartimento della persona avente diritto di firma (nome, cognome, Dipartimento/Cantone)** | **Data** **Firma** |
|---|---|
| | |

NON CLASSIFICATO

# Linee guida per l'ottenimento del certificato di LRA-Officer della Swiss Government PKI

## Spiegazioni relative all'ottenimento e all'utilizzo del certificato di LRA-Officer delle classi A e B della Swiss Government PKI (SG-PKI)

V1.0, 28.08.2018

## 1 Scopo del certificato di LRA-Officer

**Scopo**

I certificati delle classi A e B sono definiti nel quadro del modello di mercato «SD005 – modello di mercato servizio standard: gestione dell'identità e degli accessi (IAM)». I LRA-Officer sono competenti per il rilascio dei certificati delle classi A e B che possono essere utilizzati per il seguente scopo:

- rilascio, revoca e gestione dei certificati di classe A e/o B della SG-PKI.

Durante la procedura di rilascio dei certificati delle classi succitate sono eseguiti complessi meccanismi di verifica e sicurezza, che consentono di stabilire un livello di sicurezza elevato per l'identità del titolare del certificato. I certificati delle classi A e B vengono sempre consegnati personalmente e soltanto previa identificazione del titolare tramite un documento di viaggio valido per l'entrata in Svizzera.

**Scopi non ammessi**

Il certificato di LRA-Officer serve esclusivamente allo scopo sopracitato e non fornisce alcuna informazione, sicurezza o garanzia aggiuntiva. In particolare, il certificato LRA-Officer non garantiscono che il titolare stia utilizzando il certificato correttamente e legalmente. Inoltre, questo certificato non garantisce che il titolare indicato nel certificato:

- sia effettivamente coinvolto nelle attività operative;
- si attenga alle prescrizioni legali;
- sia affidabile e si comporti in modo appropriato nel contesto lavorativo.

## 2 Qualità del certificato di LRA-Officer

La SG-PKI si attiene alle procedure definite nelle direttive per la registrazione che stabiliscono quali sono i passi necessari e ragionevoli da compiere al primo rilascio di un certificato di LRA-Officer. In particolare si richiede di confermare i punti elencati di seguito:

- **esistenza giuridicamente valida:** il titolare indicato nel certificato di LRA-Officer esiste come persona fisica e i suoi dati sono reperibili in Admin-Directory;
- **identità:** il nome del titolare indicato nel certificato di LRA-Officer corrisponde a quello dell'Admin-Directory e a quello del documento di viaggio;
- **autorizzazione:** il titolare indicato nel certificato di LRA-Officer è stato autorizzato a ottenerlo dalla persona avente diritto di firma del suo ufficio;
- **esattezza dei dati:** tutti i dati e le informazioni contenuti nel certificato sono esatti;
- **condizioni contrattuali e di utilizzo:** il titolare indicato sul certificato di LRA-Officer ha letto i diritti e gli obblighi descritti nelle «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI» e dichiara di averne compreso e accettato il significato firmando l'apposito modulo di richiesta. La SG-PKI ha risposto in modo chiaro alle domande in merito poste dal LRA-Officer;
- **stato:** la SG-PKI pubblica online lo stato del certificato e le informazioni relative alla sua validità e revoca;

- **revoca:** se del caso, la SG-PKI può revocare il certificato di LRA-Officer senza preavviso in presenza di uno dei motivi citati nelle «Condizioni contrattuali e di utilizzo per i certificati di classe B».

## 3 Policy

Tutte le disposizioni legali vigenti, i criteri (compresi i CP / CPS della SG Root CA I) e le direttive per la registrazione dei certificati della SG-PKI nonché le «Condizioni contrattuali e di utilizzo per i certificati di classe B del certificato LRA-Officer della SG-PKI» e le presenti direttive sono consultabili sul sito Internet della SG-PKI (http://www.pki.admin.ch.)

Firmando il «Modulo di richiesta per LRA-Officer per certificati di classe B», l'aspirante LRA-Officer dichiara di attenersi alle direttive e alla legislazione vigente e di osservarle nell'esecuzione delle sue mansioni, in particolare:

- i CP/CPS della SG Root CA I («Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I»), in particolare gli obblighi descritti ai numeri 5.3.1 e 5.5.2;
- le «Direttive di registrazione di certificati di classe B della Swiss Government PKI»;
- le «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI»;
- le «Linee guida per l'ottenimento del certificato di LRA-Officer della Swiss Government PKI» (presente documento).

**Contenuto del certificato**

Il certificato di LRA-Officer della SG-PKI contiene informazioni riguardanti:

- l'autorità di certificazione responsabile della produzione e del rilascio;
- il certificato radice dell'autorità di certificazione responsabile del rilascio;
- le informazioni sulle policy applicate;
- la data di rilascio e di scadenza del certificato;
- il numero di serie del certificato;
- lo scopo del certificato;
- l'elenco delle revoche dei certificati (Certificate Revocation List, CRL) e sul protocollo di stato del certificato online (Online Certificate Status Protocol, OCSP);
- gli ispettori dell'autorità di certificazione;
- il titolare del certificato secondo la registrazione in Admin-Directory al momento del primo rilascio, ovvero:
    1) il common name del titolare,
    2) l'indirizzo di posta elettronica,
    3) l'UPN.

**Validità**

Il certificato di LRA-Officer della SG-PKI è valido per tre anni al massimo. Prima della scadenza, il LRA-Officer deve chiedere un nuovo certificato presso la SG-PKI e sottoporsi a una procedura analoga al primo rilascio. La SG-PKI deve provvedere al rilascio del nuovo certificato.

## 4 Ottenimento del certificato di LRA-Officer

**Ottenimento**

Per ottenere il certificato di LRA-Officer della SG-PKI sono necessari i documenti e le registrazioni indicati di seguito:

- un documento di viaggio valido per l'entrata in Svizzera (carta d'identità o passaporto), rilasciato al richiedente. L'identità è verificata dal formatore durante il corso obbligatorio per LRA-Officer;
- la registrazione in Admin-Directory che riporti cognome(i), nome(i) così come indicato nel documento di viaggio, l'indirizzo di posta elettronica valido e l'UPN (facoltativo);
- un attestato comprovante che il LRA-Officer ha seguito il corso di formazione obbligatorio per LRA-Officer e ha superato il relativo esame;
- un modulo di richiesta per LRA-Officer della SG-PKI compilato e firmato (elettronicamente) in cui:
    1) con la sua firma, l'aspirante LRA-Officer accetta:
        - la dichiarazione di confidenzialità,

- le «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI»,
- le presenti linee guida

e ordina la smart card del LRA-Officer.

2) la persona avente diritto di firma, designata dall'ufficio federale che ha assunto il LRA-Officer, con la sua firma conferma l'affidabilità dell'aspirante LRA-Officer secondo i requisiti richiesti nel modulo di richiesta per LRA-Officer al punto riguardante la verifica dell'affidabilità.

**Identificazione**

Per identificare il richiedente viene verificata la validità, l'esattezza e l'autenticità del suo documento di viaggio durante il corso di formazione per LRA-Officer. Inoltre, i formatori della SG-PKI devono accertarsi che il partecipante al corso corrisponda alla foto del documento d'identità. Infine, prima di rilasciare un certificato personale, la SG-PKI deve anche verificare la plausibilità della richiesta, accertandosi che il richiedente lavori effettivamente nell'unità organizzativa indicata in Admin-Directory, che necessiti del certificato per la sua attività quotidiana e che sia autorizzato a richiederlo.

**Carattere vincolante**

La richiesta deve essere approvata dai servizi competenti. Le presenti linee guida e le «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI» devono essere comprese dal richiedente e accettate apponendo una firma (digitale) sull'apposito modulo di richiesta.

## 5 Protezione della chiave privata e del certificato

**Trasferibilità**

Il certificato di LRA-Officer è strettamente personale e non è trasferibile. I dati personali del titolare sono salvati sia nel certificato, sia presso la SG-PKI.

**PIN e PUK**

Il PIN deve essere diverso dalle altre password e non deve essere comunicato a terzi. Non è necessario cambiarlo periodicamente, tranne che sussista il sospetto fondato che altre persone ne siano venute a conoscenza.

Per il certificato (e di conseguenza anche per i dispositivi che lo contengono come la smart card, la chiavetta USB ecc.) si deve scegliere un codice PIN di almeno sei caratteri alfanumerici o esclusivamente numerici. Per prevenire l'utilizzo illecito della propria identità elettronica, è vietato comunicare il PIN a terzi.

Il PUK della smart card deve essere costituito almeno da otto caratteri scelti secondo i criteri sopracitati.

**Obbligo di comunicazione**

Il LRA-Officer deve comunicare immediatamente l'eventuale perdita della smart card alla SG-PKI, che provvede a bloccare (ossia a revocare) il certificato in questione e a pubblicarne il blocco in un apposito elenco pubblico disponibile online. Il certificato rimane bloccato, e quindi non valido, anche se la smart card viene ritrovata. Subito dopo il blocco è possibile presentare la richiesta per l'ottenimento di un nuovo certificato di LRA-Officer presso la SG-PKI. La procedura per il rilascio di una nuova smart card avviene secondo le stesse modalità del primo rilascio.

In caso di modifica della persona giuridica, del cognome (ad es. dopo il matrimonio) o dell'indirizzo di posta elettronica deve essere rilasciato un nuovo certificato (primo rilascio).

## 6 Revoca

Per ottenere una revoca si deve inviare una richiesta alla SG-PKI. A tal fine le persone autorizzate (v. elenco esaustivo sottostante) possono scaricare l'apposito modulo sulla homepage del sito Internet della SG-PKI (hwww.pki.admin.ch). Se invece la revoca viene richiesta telefonicamente, la SG-PKI identifica il richiedente mediante la passphrase di revoca e i dati personali (data, luogo di nascita ecc.). La richiesta telefonica è riservata esclusivamente al richiedente, mentre le altre persone autorizzate possono farlo soltanto per iscritto.

Le persone autorizzate sono:

- il titolare del certificato;
- il responsabile della SG-PKI;
- il responsabile della sicurezza della SG-PKI;
- le persone competenti del titolare del certificato in questione:
  - il collaboratore RU (Servizio del personale),
  - il superiore diretto,
  - il LRA-Officer,
  - l'ISIU,
  - l'ISID,
  - il responsabile PKI all'interno dell'unità organizzativa.

## 7 Contenuto del certificato

***Certificato di autenticazione (chiave di autenticazione)***
Impronta digitale (SHA-1):
Validità del certificato:
Numero di serie:

## 8 Accettazione e conferma di ricezione della smart card

Firmando il modulo per la conferma di ricezione del certificato di LRA-Officer, dopo aver ricevuto la smart card il titolare conferma:

- l'esattezza dei dati salvati nel certificato;
- l'avvenuta consegna della smart card;
- di aver compreso e accettato le presenti linee guida nonché i diritti e gli obblighi che ne derivano; conferma inoltre che la SG-PKI ha risposto in modo chiaro ad eventuali domande;
- di aver compilato correttamente la passphrase di revoca e gli altri campi necessari per identificare telefonicamente la persona e individuare il certificato.

Inoltre l'aspirante LRA-Officer si impegna ad osservare le direttive esposte nel presente documento e descritte nel CP/CPS, ad adempiere i requisiti e a svolgere i compiti descritti nelle «Direttive per la registrazione dei certificati di classe B della Swiss Government PKI».

Per ulteriori informazioni contattare la SG-PKI all'indirizzo pki-info@bit.admin.ch.

NON CLASSIFICATO

# Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI

## Per il rilascio dei certificati personali di classe A (qualificati e regolati) e B (avanzati) della Swiss Government PKI (SG-PKI) e delle autorità federali della Confederazione Svizzera

V1.0 28.08.2018

Nel suo ruolo di Trust Service Provider (TSP), la SG-PKI dell'UFIT gestisce, su incarico dell'Organo direzione informatica della Confederazione (ODIC), le infrastrutture a chiave pubblica (Public Key Infrastructure, PKI) delle autorità federali della Confederazione Svizzera. I certificati delle classi A e B sono definiti nel quadro del modello di mercato «SD005 – modello di mercato servizio standard: gestione dell'identità e degli accessi (IAM)». I LRA-Officer sono competenti per il rilascio dei certificati delle classi A e B. L'ottenimento e l'utilizzo dei certificati di LRA-Officer per il rilascio di certificati delle classi A e B della SG-PKI sottostanno alle disposizioni delle condizioni contrattuali e di utilizzo per i certificati di classe A e B. Ogni anno la SG-PKI adegua le presenti condizioni alle disposizioni legali vigenti e ai requisiti normativi definiti per le infrastrutture a chiave pubblica. Questi ultimi fungono da base per le presenti condizioni contrattuali e di utilizzo. La versione in vigore è pubblicata su www.pki.admin.ch. I titolari dei certificati vengono informati per e-mail in merito alla pubblicazione della versione aggiornata dei documenti.
Si deve inoltre tenere conto delle «Linee guida per l'ottenimento del certificato di LRA-Officer della Swiss Government PKI», che devono essere accettate separatamente al momento del rilascio di un certificato di LRA-Officer.

**Esattezza e completezza delle informazioni**

Il titolare di un certificato LRA-Officer della SG-PKI (di seguito «titolare» o LRA-Officer[4]) si impegna a fornire al TSP informazioni esatte ed esaustive per la procedura concernente il rilascio e il contenuto del certificato. Prima di rilasciare un certificato LRA-Officer, il titolare deve essere identificato di persona sulla base di un documento di viaggio valido. Il certificato è indissolubilmente legato al LRA-Officer e il suo nome, cognome, suffisso e indirizzo e-mail vengono sempre indicati nel certificato.

Il titolare si impegna a verificare i dati personali dei suoi clienti (= titolari di certificati di classe A e/o B) conformemente alle «Direttive per la registrazione dei certificati di classe A/B della Swiss Government».

Il LRA-Officer è tenuto a comunicare al TSP qualsiasi cambiamento dei propri dati personali, in particolare se riguarda nome, cognome, suffisso (registrazione in Admin-Directory) o indirizzo di posta elettronica.

**Protezione della chiave privata e del certificato**

Il LRA-Officer si impegna ad adottare tutte le misure necessarie per garantire il controllo esclusivo, la confidenzialità e la protezione contro la perdita e l'utilizzo illecito della chiave privata e dei dati di attivazione (ad es. PIN, PUK) e dei dispositivi eventualmente collegati (ad es. smart card). La chiave privata del certificato può e deve essere impiegata soltanto unitamente al certificato stesso e unicamente per gli scopi (rilascio, revoca, gestione dei certificati delle classi A e B) stabiliti nel certificato. In nessun caso può essere resa accessibile a terzi non autorizzati. Il titolare risponde per qualsiasi danno causato dalla trasmissione a terzi della chiave privata e degli eventuali dati di attivazione e dispositivi collegati.

Il TSP si riserva di revocare il certificato senza preavviso, anche in presenza di un sospetto concreto di utilizzo illecito o di accesso non autorizzato alla chiave privata.

[4] I termini di genere maschile nel presente documento si riferiscono a persone di entrambi i sessi.

**Utilizzo del certificato**

Il LRA-Officer garantisce di conoscere il contenuto, lo scopo e l'effetto dell'utilizzo del certificato di LRA-Officer. Inoltre si impegna a utilizzare il certificato disponibile sulla smart card e la relativa chiave privata esclusivamente per le operazioni autorizzate e nel rispetto delle prescrizioni legali vigenti come pure delle disposizioni delle presenti direttive.

**Comunicazione e revoca**

Il LRA-Officer si impegna a cessare immediatamente l'utilizzo di certificati e delle relative chiavi private e a chiederne la revoca al TSP se:

- sussiste il sospetto concreto che un certificato sia stato usato per attività dubbie (utilizzo illecito dei dati di attivazione);
- le informazioni contenute nel certificato non sono aggiornate o esatte o non lo saranno più entro breve.

In caso di sospetto di compromissione o utilizzo illecito dei certificati, è necessario seguire immediatamente le istruzioni del TSP.

Se richiesto per motivi di sicurezza e se ammesso dal punto di vista della protezione dei dati, il TSP può trasmettere ad altri servizi competenti, ad altri TSP nonché a imprese e gruppi industriali i dati concernenti il titolare, il certificato e altre informazioni direttamente correlate, se il certificato o la persona che lo usa vengono identificati come fonti di un utilizzo illecito.

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

**Fine dell'utilizzo del certificato**

Alla scadenza della validità o dopo la revoca del certificato (in particolare a causa di una sua compromissione) il LRA-Officer si impegna a cessarne immediatamente l'utilizzo.

**Responsabilità**

Il LRA-Officer è responsabile affinché il certificato di LRA-Officer e la relativa chiave privata siano utilizzati soltanto nel rispetto delle disposizioni al numero «Utilizzo del certificato» del presente documento. Una violazione di queste norme comporta la revoca e altre misure di natura amministrativa ed eventualmente giuridica. Il LRA-Officer è responsabile di tutte le operazioni svolte sulla sua smart card nonché di eventuali danni e conseguenze derivanti da un uso non consentito.

**Dichiarazione di riconoscimento e di consenso**

Il LRA-Officer prende atto del fatto che il TSP revoca immediatamente il certificato già in caso di sospetto fondato di utilizzo illecito, di violazione delle disposizioni contenute nel presente documento o di qualsiasi altra violazione delle disposizioni legali vigenti.

Apponendo la firma nel corrispondente modulo di richiesta, il LRA-Officer conferma di aver letto e compreso il presente documento «Condizioni contrattuali e di utilizzo per LRA-Officer della Swiss Government PKI» e di accettarne le disposizioni ivi contenute.

NON CLASSIFICATO

# Condizioni contrattuali e di utilizzo per i certificati di classe B

## Per i certificati di firma personali e avanzati della Swiss Government PKI (SG-PKI) delle autorità federali della Confederazione Svizzera

V1.1, 31.03.2017

Nel suo ruolo di Certification Service Provider (CSP), la SG-PKI dell'UFIT gestisce, su incarico dell'Organo direzione informatica della Confederazione (ODIC), le infrastrutture a chiave pubblica (Public Key Infrastructure, PKI) delle autorità federali della Confederazione Svizzera. I certificati di classe B sono definiti nel quadro del modello di mercato «SD005 – modello di mercato servizio standard: gestione dell'identità e degli accessi (IAM)». L'ottenimento e l'utilizzo dei certificati di classe B della SG-PKI sottostanno alle disposizioni delle presenti condizioni contrattuali e di utilizzo. Ogni anno la SG-PKI adegua le presenti condizioni alle disposizioni legali vigenti e ai requisiti normativi definiti per le infrastrutture a chiave pubblica. Questi ultimi fungono da base per le presenti condizioni contrattuali e di utilizzo. La versione in vigore è pubblicata su www.pki.admin.ch. I titolari dei certificati vengono informati per e-mail in merito alla pubblicazione della versione aggiornata dei documenti.

Si deve inoltre tenere conto delle «Linee guida della SG-PKI per i certificati di classe B», che devono essere accettate separatamente all'atto della consegna.

**Esattezza e completezza delle informazioni**

Il titolare di certificati di classe B della SG-PKI (di seguito «titolare»[5]) si impegna a fornire al CSP informazioni esatte ed esaustive ai fini della procedura di rilascio e del contenuto del certificato. Prima del rilascio del certificato, il cliente deve essere identificato di persona sulla base di un documento di viaggio valido. Il certificato è indissolubilmente legato al cliente.

Nel certificato figurano sempre nome(i), cognome(i), suffisso e indirizzo e-mail del cliente. Presso la SG-PKI vengono registrati altri dati personali del titolare, quali le passphrase di revoca e la scansione del documento di viaggio valido.

Il cliente comunica al CSP qualsiasi cambiamento dei propri dati personali, qualsiasi cambiamento dei propri dati personali, in particolare se riguarda nome, cognome, suffisso (registrazione in Admin-Directory) o indirizzo di posta elettronica.

**Protezione della chiave privata e del certificato**

Il titolare si impegna a prendere tutte le misure necessarie a garantire il controllo esclusivo, la confidenzialità e la protezione contro la perdita e l'utilizzo illecito delle chiavi private e degli eventuali dati di attivazione (ad es. PIN, PUK) e dei dispositivi pertinenti (ad es. smart card). La chiave privata del certificato può e deve essere impiegata soltanto unitamente al certificato stesso e unicamente per lo scopo (firma, autenticazione, crittografia) stabilito nel certificato. Non è consentito per nessun motivo renderla accessibile a terzi non autorizzati.

Il CSP si riserva di revocare il certificato senza preavviso, anche in presenza di un sospetto concreto di utilizzo illecito o di accesso non autorizzato alle chiavi private.

**Utilizzo del certificato**

l titolare garantisce di conoscere il contenuto, lo scopo e l'effetto dell'utilizzo dei certificati di classe B. Inoltre si impegna a utilizzare i certificati di classe B e la relativa chiave privata esclusivamente per le operazioni autorizzate e nel rispetto delle prescrizioni legali vigenti, nonché delle disposizioni contenute del presente documento.

[5] I termini di genere maschile nel presente documento si riferiscono a persone di entrambi i sessi.

**Comunicazione e revoca**

Il titolare si impegna a cessare immediatamente l'utilizzo dei certificati e delle relative chiavi private e a chiederne la revoca al CSP se:

- sussiste il sospetto concreto che un certificato sia stato impiegato per attività dubbie (abuso dei dati di attivazione, del certificato di firma o del certificato di crittografia);
- le informazioni contenute nel certificato non sono aggiornate o esatte o non lo saranno più entro breve.

In caso di sospetto di compromissione o utilizzo illecito dei certificati, è necessario seguire immediatamente le istruzioni 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 nonché a imprese e gruppi industriali i dati concernenti il titolare, il certificato e altre informazioni direttamente correlate, se il certificato o la persona che lo usa vengono identificati come fonti di un utilizzo illecito.

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

**Fine dell'utilizzo del certificato**

Alla scadenza della validità o dopo la revoca dei certificati (in particolare a causa di una loro compromissione) il titolare si impegna a cessarne immediatamente l'utilizzo.

**Responsabilità**

Il titolare è responsabile affinché il certificato di classe B e le relative chiavi private siano utilizzati soltanto nel rispetto delle disposizioni al numero «Utilizzo del certificato» del presente documento. Una violazione di queste norme comporta la revoca e altre misure di natura amministrativa e, se del caso, giuridica. Il titolare è responsabile di tutte le firme da lui apposte, delle autenticazioni e delle crittografie nonché di eventuali danni e conseguenze derivanti da un utilizzo irregolare.

**Dichiarazione di riconoscimento e di consenso**

Il titolare prende atto del fatto che il CSP revoca immediatamente i certificati anche in caso di un sospetto fondato di utilizzo illecito, di inosservanza delle prescrizioni del presente documento o di un'altra violazione delle disposizioni legali vigenti.

Il titolare conferma con la propria firma di aver letto e compreso il presente documento («Condizioni contrattuali e di utilizzo per i certificati di classe B») e di accettarne le disposizioni ivi contenute.

Luogo e data: _____ Firma: _____

NON CLASSIFICATO

# Linee guida della Swiss Government PKI per i certificati di classe B

## Spiegazioni relative all'ottenimento e all'utilizzo dei certificati di classe B della Swiss Government PKI (SG-PKI)

V1.0, 09.03.2017

## 1 Scopo dei certificati di classe B

**Scopo**

I certificati di classe B sono definiti nel quadro del modello di mercato «SD005 – modello di mercato servizio standard: gestione dell'identità e degli accessi (IAM)». I certificati di classe B possono essere utilizzati per i seguenti scopi:

- firma attendibile di dati per garantire la loro autenticità e integrità;
- crittografia dei dati per garantirne la confidenzialità;
- autenticazione di persone: il certificato fornisce al titolare un'identità digitale protetta per la verifica di elementi importanti (ad es. per accedere ai vari portali).

Durante la procedura di rilascio dei certificati di classe B vengono messi in atto complessi meccanismi di verifica e sicurezza con i quali si stabilisce un livello di sicurezza elevato per l'identità del titolare del certificato. I certificati di classe B vengono sempre consegnati di persona e soltanto previa identificazione del titolare tramite un documento d'identità valido per entrare in Svizzera.

**Scopi non ammessi**

I certificati di classe B servono esclusivamente agli scopi sopracitati e non forniscono alcuna informazione, sicurezza o garanzia aggiuntiva. In particolare, i certificati di classe B non garantiscono che il titolare stia utilizzando il certificato correttamente e legalmente. Inoltre, i certificati di classe B non garantiscono che il titolare indicato nel certificato:

- sia effettivamente coinvolto nelle attività operative;
- si attenga alle prescrizioni legali;
- sia affidabile e si comporti in modo appropriato nel contesto lavorativo;
- possieda le competenze professionali, tecniche, organizzative o di altro genere per utilizzarlo correttamente.

## 2 Qualità dei certificati di classe B

Il LRA-Officer della SG-PKI si attiene alle procedure definite nelle «Direttive di registrazione di certificati di classe B della Swiss Government PKI», che stabiliscono quali sono i passi necessari e ragionevoli da compiere al primo rilascio di un certificato di classe B. In particolare si richiede di confermare i punti elencati di seguito:

- **esistenza giuridicamente valida:** il titolare indicato nel certificato di classe B esiste come persona fisica e i suoi dati sono reperibili in Admin-Directory;
- **identità:** il nome del titolare indicato nel certificato di classe B coincide con quello riportato sul suo documento di viaggio valido;
- **autorizzazione:** il titolare indicato nel certificato di classe B è stato autorizzato ad ottenerlo;
- **esattezza dei dati:** tutti i dati e le informazioni contenuti nel certificato sono esatti;
- **condizioni contrattuali e di utilizzo:** il LRA-Officer ha informato il titolare indicato nel certificato di classe B dei suoi diritti e obblighi riportati nelle «Condizioni contrattuali e di utilizzo per i certificati di classe B» e ha risposto chiaramente alle sue eventuali domande in merito. Il titolare ha letto, accettato e firmato le condizioni suddette;

- **stato:** la SG-PKI pubblica online lo stato del certificato e le informazioni relative alla sua validità e revoca;
- **revoca:** se del caso, la SG-PKI può revocare il certificato di classe B senza preavviso in presenza di uno dei motivi citati nelle «Condizioni contrattuali e di utilizzo per i certificati di classe B».

## 3 Policy

Tutte le vigenti disposizioni legali, i criteri (compresi i CP/CPS) e le direttive concernenti i certificati di classe B sono consultabili sul sito della SG-PKI (www.pki.admin.ch.).

## 4 Contenuto e validità del certificato di classe B

### Contenuto del certificato

Il certificato di classe B della SG-PKI contiene informazioni riguardanti:

- l'autorità di certificazione responsabile della produzione e del rilascio;
- le informazioni sulla CA radice e la CA emittente;
- le informazioni sulle policy applicate;
- la data di rilascio e di scadenza del certificato;
- il numero di serie del certificato;
- l'utilizzo del certificato;
- l'elenco delle revoche dei certificati (Certificate Revocation List, CRL) e sul protocollo di stato del certificato online (Online Certificate Status Protocol, OCSP);
- gli ispettori dell'autorità di certificazione;
- il titolare del certificato secondo la registrazione in Admin-Directory al momento del primo rilascio, ovvero:
    1) il common name del titolare,
    2) l'indirizzo di posta elettronica,
    3) l'UPN.

### Validità

Il certificato di classe B della SG-PKI è valido per tre anni al massimo. Prima della scadenza triennale, il titolare del certificato può presentare richiesta di rinnovo triennale al massimo due volte utilizzando il rekeying wizard. Alla scadenza del periodo di validità triennale, il LRA-Officer dovrà rilasciare un nuovo certificato seguendo la stessa procedura del primo rilascio.

## 5 Ottenimento dei certificati di classe B

### Ottenimento

Per ottenere i certificati di classe B della SG-PKI sono necessari i documenti e le registrazioni elencate di seguito:

- un documento di viaggio valido per entrare in Svizzera (carta d'identità o passaporto), rilasciato al richiedente;
- un modulo per la richiesta di certificati di classe B della SG-PKI compilato e firmato (elettronicamente) oppure la registrazione del richiedente da parte di un superiore nell'UA o tramite la procedura stabilita internamente dalle RU della UA;
- le «Condizioni contrattuali e di utilizzo per i certificati di classe B» firmate, che vengono sempre stampate con il presente documento da un LRA-Officer al momento del rilascio;
- la registrazione in Admin-Directory che riporti cognome(i), nome(i) così come indicato nel documento di viaggio, l'indirizzo di posta elettronica valido e l'UPN (facoltativo).

### Identificazione

L'identificazione personale del richiedente viene effettuata dai LRA-Officer di classe B della SG-PKI al momento del primo rilascio o al più tardi dopo la scadenza del terzo periodo di validità. Nel caso in cui i certificati di classe B vengano rilasciati fuori sede, l'identificazione personale viene effettuata dal RIO (Registration Identification

Officer), che agisce in vece del LRA-Officer e gli inoltra la conferma di avvenuta identificazione ai fini dell'approvazione della richiesta.

Per identificare il richiedente vengono verificate la validità, la correttezza e l'autenticità del suo documento di viaggio. Inoltre, i LRA-Officer devono accertarsi che il richiedente corrisponda effettivamente alla foto riportata sul suo documento di viaggio. Infine, prima di rilasciare un certificato, dovranno anche verificare l'attendibilità della richiesta, accertandosi che il richiedente lavori effettivamente presso l'unità organizzativa indicata in Admin-Directory, necessiti del certificato per la sua attività lavorativa quotidiana e sia autorizzato a richiederlo.

**Carattere vincolante della richiesta**

La richiesta (o la procedura interna per avviarla) deve essere approvata dai servizi competenti. Le presenti linee guida e le «Condizioni contrattuali e di utilizzo per i certificati di classe B» devono essere accettate e firmate (elettronicamente) dal richiedente.

## 6 Protezione della chiave privata e del certificato

**Trasferibilità**

Il certificato di classe B è strettamente personale e non è trasferibile. I dati personali del titolare sono salvati nel certificato e dalla SG-PKI.

**PIN e PUK**

Il PIN deve essere diverso dalle altre password e non deve essere comunicato a terzi. Non è necessario cambiarlo periodicamente, a meno che non sussista il sospetto fondato che altre persone ne siano venute a conoscenza.

Per il certificato (e di conseguenza anche per i dispositivi che lo contengono come la smart card, la chiavetta USB ecc.) si deve scegliere una password di almeno sei caratteri alfanumerici o esclusivamente numerici. Per prevenire l'utilizzo illecito della propria identità elettronica, il PIN non deve mai essere comunicato a terzi.

Il PUK della smart card deve essere costituito almeno da otto caratteri scelti secondo i criteri sopracitati.

**Obbligo di comunicazione**

Il titolare deve comunicare immediatamente l'eventuale perdita della smart card al LRA-Officer o al servizio di supporto informatico competente, che provvede a bloccare (ossia a revocare) il certificato in questione e a pubblicarne il blocco in un apposito elenco pubblico disponibile online. Il certificato rimane bloccato, e quindi non valido, anche nel caso in cui la smart card venga ritrovata. Una volta che il certificato di classe B è stato bloccato, è possibile richiederne uno nuovo LRA-Officer competente. La procedura di rilascio si svolge secondo le stesse modalità del primo rilascio.

In caso di modifica della persona giuridica, del cognome (ad es. dopo il matrimonio) o dell'indirizzo di posta elettronica deve essere rilasciato un nuovo certificato (primo rilascio).

## 7 Revoca

Per ottenere una revoca bisogna inoltrare una richiesta al LRA-Officer: a tal fine le persone autorizzate (v. elenco sottostante, da considerarsi esaustivo) possono scaricare i moduli necessari dalla pagina iniziale della SG-PKI www.pki.admin.ch alla voce «Certificate Revocation List». Se invece la revoca viene richiesta telefonicamente, il LRA-Officer identificherà il richiedente durante la telefonata mediante la passphrase di revoca e i dati personali (data e luogo di nascita ecc.). La richiesta telefonica è riservata esclusivamente al richiedente, mentre le altre persone autorizzate possono farlo soltanto per iscritto.

Le persone autorizzate sono:

- il titolare del certificato;
- il responsabile della SG-PKI;
- il responsabile della sicurezza della SG-PKI;

- le persone competenti del titolare del certificato in questione:
  - i collaboratori RU (Servizio del personale),
  - i superiori diretti,
  - il LRA-Officer,
  - l'ISIU,
  - l'ISID,
  - il responsabile PKI all'interno dell'unità organizzativa.

## 8 Contenuto del certificato

***Certificato di autenticazione (chiave di autenticazione)***
Impronta digitale (SHA-1):
Validità del certificato:
Numero di serie:

***Certificato di crittografia (chiave di crittografia)***
Impronta digitale (SHA-1):
Validità del certificato:
Numero di serie:

***Certificato di firma (chiave di firma)***
Impronta digitale (SHA-1):
Validità del certificato:
Numero di serie:

## 9 Accettazione e conferma di ricezione della smart card

Con la propria firma, il titolare conferma:

- la correttezza dei dati salvati nel certificato;
- l'avvenuta consegna della smart card;
- di aver letto e discusso con il LRA-Officer le presenti linee guida. Il LRA-Officer ha risposto in modo chiaro alle domande;
- di aver compreso e accettato i suoi diritti e obblighi spiegati nelle presenti linee guida;
- di attuare le direttive ivi descritte.

Per ulteriori informazioni contattare la SG-PKI all'indirizzo pki-info@bit.admin.ch[6].

**Common name (CN):**

**Data di rilascio:** **Firma:** _____

[6] Si prega di leggere anche le «Condizioni contrattuali e di utilizzo per i certificati di classe B». Nell'ordinazione del proprio certificato di classe B è richiesta una copia firmata digitalmente di questo documento (www.pki.admin.ch).

# Allegato C: storico delle modifiche

| Versione | Oggetto della modifica | Riferimento, numero |
|---|---|---|
| **V5.2** | Definizioni, acronimi e abbreviazioni: diversi complementi e correzioni | Definizioni, acronimi e abbreviazioni |
| **V5.2** | Aggiunti i riferimenti [29]–[32]. | Documenti di riferimento |
| **V5.2** | Precisazione: i certificati di classe B sono rilasciati esclusivamente a persone fisiche | 1.3 |
| **V5.2** | Controllo di sicurezza relativo alle persone: l'ufficio che ha assunto la persona chiede un controllo di sicurezza relativo alle persone o una verifica dell'affidabilità | 2.1, 3.13 |
| **V5.2** | D'ora in poi, il supporto fornito ai LRA-Officer avviene tramite il Service Desk UFIT, un Remedy Ticket o una richiesta MAC | 3.2, 3.11, 3.12 |
| **V5.2** | Controllo degli accessi: ridefiniti i requisiti sulle ubicazioni dei LRA-Office | 3.3 |
| **V5.2** | Controllo degli accessi: i requisiti inerenti alla protezione del PC dei LRA-Officer sono stati adeguati ai requisiti di BAB client | 3.4, 3.5 |
| **V5.2** | Moduli e dati dei clienti: precisazione relativa alla loro conservazione | 3.6 |
| **V5.2** | Registro: nuove direttive per la tenuta del registro (elettronico) e regolamento relativo agli accessi | 3.7 |
| **V5.2** | Precisazioni sull'accesso (elettronico) sicuro e termini di conservazione per i documenti in formato elettronico | 3.8, 3.9 |
| **V5.2** | Certificato speciale per LRA-Officer sostituito da autorizzazioni per il rilascio di certificati di classe B personali | 3.10 |
| **V5.2** | Protezione delle chiavi private della postazione LRA | Eliminato il n. 3.10 |
| **V5.2** | Postazione LRA sostituita da BAB client con funzioni di LRA-Officer | 3.11, 3.12 |
| **V5.2** | Precisazioni relative alla legislazione vigente in materia di protezione dei dati personali | 3.14 |
| **V5.2** | Precisazioni relative alla formazione e alla formazione continua dei LRA-Officer; correzioni e indicazioni riguardanti il punteggio richiesto | 3.15, 3.16 |
| **V5.2** | Reset del PIN e gestione del PUK | Nuovo: n. 3.19 |
| **V5.2** | Verifica di conformità: testo rielaborato | 4 |
| **V5.2** | Procedura senza RIO: aggiunte relative alla procedura di rilascio per richiedenti con permesso F | 5.2, 5.2.3.2, 5.2.3.7, 5.2.4.2 |
| **V5.2** | Registrazione dei mandati per il rilascio di certificati nel sistema di registrazione dei mandati (MAC, Gever) e convalida dell'identificazione tramite il permesso F, modulo aggiuntivo incluso | 5.2.2, 5.2.3.2 |
| **V5.2** | Aggiunta dei campi 4 e 5 («adminGivenNameLong» e «adminSurNameLong») nell'Admin-Directory e nel tool del LRA-Officer; introduzione dei possibili varianti decisionali per il rilascio di certificati | 5.2.3.1 |
| **V5.2** | Inclusione dei documenti d'identità nella procedura di scansione | 5.2.3.7 |
| **V5.2** | Gestione dei dati e archiviazione elettroniche (file di scansione) | 3.7, 3.8, 5.2.3.6, 5.2.3.8, 5.2.3.12, 5.2.3.13 |
| **V5.2** | Revoca: precisazione nel caso dell'identificazione per telefono | 5.3.2 |
| **V5.2** | Modulo di revoca: nuove direttive in caso di revoca tramite il revoke wizard | 5.3.4.2, 5.3.4.4, 6.3 |
| **V5.2** | Moduli rilevanti ai fini della verifica: menzionata la rilevanza nel capitolo pertinente | 6.1 segg. |
| **V5.2** | Modulo di richiesta: adeguati i requisiti concernenti i dati richiesti | 6.1 |
| **V5.2** | Nuove direttive inerenti alla conferma di ricezione della smart card | 6.2 |
| **V5.2** | Modulo di richiesta complementare per i richiedenti con permesso F | Nuovo n. 6.1.1 |
| **V5.2** | Liste di controllo: diverse correzioni | Allegato A |
| **V5.2** | Moduli: vari aggiornamenti e correzioni nonché nuovo modulo per richiedenti con permesso F | Allegato B |

| | | |
|---|---|---|
| **V5.2** | Moduli: per completezza, aggiunti i moduli del LRA-Officer, dell'Amministrazione federale e della direzione | Allegato B |
| **V5.2** | Storico delle modifiche, stato versione ed entrata in vigore del documento | Nuovo allegato C |
| **V5.2** | Adeguamento liste di controllo e moduli | Allegato B |
| **V5.2** | Integrazione nelle direttive di registrazione del modulo di reset del PIN per superuser e del modulo di richiesta per il Key Recovery Agent | Allegato B |
| **V5.9** | Modifica del controllo di versione prima dell'approvazione | V5.2 direttive |
| **V5.9** | Eliminato il n. 3.12. | Già 3.12 |
| **V6.0** | Controllo di versione dopo la validazione | Controllo di versione |

Stato versione 6.0: 01.11.2019

Entrata in vigore della versione tedesca: 01.01.2020