Direttive per la registrazione dei certificati qualificati e regolamentati di classe A della Swiss Government PKI

Direttive destinate ai LRA-Officer per il rilascio e la gestione dei certificati qualificati e regolamentati di classe A con certificato di firma per persone fisiche e giuridici secondo la FiEle

V1.0, 18.05.2026

Classificazione	Generale
Stato	Approvato
Nome del progetto	Direttive per la registrazione dei certificati qualificati e regolamentati di classe A della Swiss Government PKI
Committente	Swiss Government PKI
Autore	Swiss Government PKI
Elaborato da	Salvatore Tomasulo, Stefan Good, Silvio Pelli, Cornelia Enke, Mario Lovisi
Verificato da	Product Owner e Security Officer SG-PKI
Autorizzato da	Product Owner TRS e Security Officer SG-PKI
Distribuzione	LRA-Officer, ispettori
Doc_ID	0239-RV-Direttive per la registrazione dei certificati qualificati e regolamentati di classe A della Swiss Government PKI-i
Breve descrizione	Le presenti direttive descrivono le procedure che i LRA-Officer devono seguire per il rilascio e la gestione dei certificati di classe A qualificati e regolamentati. Esse precisano le disposizioni indicate nei certificati radice CP/CPS dell'autorità di certificazione (Issuing e Root).
Luogo di archiviazione	ActaNova: 422-SERV/SIGVALD

Controllo delle modifiche, verifica e approvazione

Versione	Data	Descrizione/Osservazioni	Collaboratore/Ruolo
1.0	18.05.2026	Unificazione in un unico documento delle linee guida di registrazione per i certificati di classe A – certificati qualificati e certificati di autorità regolamentati	Salvatore Tomasulo / Silvio Pelli / Mario Lovisi

Approvazione

Versione	Data	Nome	Ruolo
1.0	18.05.2026	Lovisi Mario Weber Jürgen	Product Owner Security Officer

Definizioni, acronimi e abbreviazioni

Termine/Abbreviazione	Definizione
Admin-Directory	Admin-Directory è un repertorio dell'Amministrazione federale in cui sono registrati, tra l'altro, i certificati e gli elenchi dei certificati revocati, accessibili agli utenti finali. Si tratta di un repertorio predisposto conformemente alla raccomandazione X.500.
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).
CP/CPS	Certificate Policy e Certificate Practice Statement: documenti che descrivono i modelli e i processi per il rilascio e la gestione dei certificati emessi dalla CA descritta.
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.
CSP	Certificate Service Provider (fornitore di servizi di certificazione): organizzazione che gestisce una PKI, ad esempio la 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.
Certificato regolamentato	Un certificato rilasciato ai sensi delle disposizioni della FiEle a favore di una persona giuridica della pubblica amministrazione.
Classi di certificati	La SG-PKI rilascia certificati delle classi A, B e C tramite diverse CA dall'infrastruttura a chiave pubblica (PKI) nell'Amministrazione federale [7].
Dati di attivazione	Dati che un utente deve inserire per attivare un modulo crittografico (ad es.smartcard). Le chiavi private non sono considerate dati di attivazione.
Dossier clienti	Un dossier cliente è l'archivio LRA dei documenti e delle prove raccolti dall'LRA in occasione di ogni emissione, revoca o movimento. I dossier clienti devono essere conservati per 11 anni. I dossier clienti possono essere conservati in forma cartacea (raccoglitori, archivi) o elettronica (secondo determinate regole).

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: 1. se la chiave utilizzata per codificare il messaggio è quella del firmatario; 2. se dopo la codifica il messaggio è stato modificato.
Issuing CA	Certification Authority (autorità di certificazione): parte integrante di una PKI che rilascia certificati attraverso la firma dei dati di cifratura applicando una policy definita.
Legge sulla firma elettronica (FiEle)	Legge federale del 18.3.2016 sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (RS *943.03*).
Local Registration Authority (LRA)	Un LRA è una persona o un'organizzazione responsabile dell'identificazione e della verifica dell'idoneità di un richiedente o di un titolare di certificato. Un LRA non firma né rilascia il certificato. L'LRA si fa conferire determinati compiti dalla CA. I compiti dell'LRA vengono svolti dai funzionari LRA. Oltre all'hardware (laptop) e al software (client LRA) utilizzati per l'elaborazione dei certificati, ciò comprende in particolare anche i locali in cui vengono identificati i clienti, rilasciati i certificati, conservati i dossier dei clienti e gestiti i computer dell'LRA. Nel caso dei certificati regolamentati delle autorità, l'LRA fa parte dell'organizzazione della Swiss Government PKI.
LRA-Officer (LRAO)	Persona che opera su mandato della SG-PKI e svolge i compiti che incombono alla LRA, ad esempio l'identificazione dei clienti, l'elaborazione o la revoca dei certificati.
Object Identifier (OID)	Identificativo numerico univoco attribuito a un oggetto o a una categoria di oggetti conformemente alle norme internazionali.
Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)	Ordinanza del 4 marzo 2011 sui controlli di sicurezza relativi alle persone (stato 1.9.2017).
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.
Public Key Infrastructure (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.
Richiedente	Persona che presenta una richiesta di certificato. Dopo il rilascio, la persona viene definita titolare del certificato.
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).
Servizio di firma TW4S	Trustworthy Systems Supporting Server Signing (TW4S) indica un framework sicuro e una serie di specifiche tecniche per la firma digitale centralizzata e basata su server. Consente agli utenti di creare da remoto firme elettroniche qualificate o sigilli regolamentati, mantenendo il controllo esclusivo sulle proprie chiavi di firma.
Swiss Government PKI (SG-PKI)	Infrastruttura dell'UFIT per le classi di certificati proposte nel servizio standard.

Termine/Abbreviazione	Definizione
Swiss Government Regulated CA 03	Autorità di certificazione che rilascia i certificati di classe A qualificati e regolamentati per le autorità.
Titolare del certificato (di classe A della SG-PKI)	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).
TSP	Trust Service Provider All'interno dell'amministrazione federale, si tratta dell'UFIT.
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.
Valore hash, impronta digitale	Un valore hash è un valore numerico generato da un determinato input di dati mediante l'applicazione di un cosiddetto algoritmo hash. Poiché un buon algoritmo produce valori hash diversi per dati diversi, esso funge anche da "impronta digitale" per garantire la trasmissione autentica dei documenti. In caso di falsificazione, il valore hash calcolato dal destinatario non corrisponderebbe più a quello inviato dal mittente. Il valore hash crittografato con la chiave segreta del mittente è denominato firma digitale.

Documenti di riferimento

Simbolo	Titolo, fonte
[1]	**Swiss Government PKI - Root CA IV - CP_CPS EN** (0261-RV-CP-CPS Root_CA_IV_(2.16_756_1_17_3_5_0) la versione attualmente pubblicata Fonte: SG-PKI
[2]	**Legge del 18.3.2016 sulla firma elettronica (FiEle, RS *943.03*)** Versione del 18.03.2016 (stato del 1.1.2020)Fonte : https://www.fedlex.admin.ch/eli/cc/2016/752/it
[3]	**Ordinanza del 23.11.2016 sulla firma elettronica (OFiEle, RS *943.032*)** Versione: del 23.11.2016 (stato del 1.11.2025)Fonte: https://www.fedlex.admin.ch/eli/cc/2016/753/it
[4]	**Ordinanza dell'UFCOM del 23.11.2016 sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (RS *943.032.1*)** Versione: del 23.11.2016 (stato del 1.11.2025)Fonte: https://www.fedlex.admin.ch/eli/cc/2016/754/it
[5]	**Condizioni contrattuali e di utilizzo per i certificati di classe A -Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)** (0094-RV-Terms and Conditions Class A - qualified.docx) Versione la versione attualmente pubblicata Fonte: SG-PKI
[6]	**120.4 Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)** Versione : del 04.03.2011 (stato del 01.09.2023Fonte: https://www.fedlex.admin.ch/eli/cc/2011/155/it
[7]	**120.73 Ordinanza sulla protezione contro i ciber-rischi nell'Ammisnstrazione federale** Entrata in vigore: 27.05.2020 (stato: 01.04.2021) Fonte: ODIC, https://www.fedlex.admin.ch/eli/cc/2020/416/it

Simbolo	Titolo, fonte
[8]	**IETF RFC 1309: ITU-T X.500 Technical Overview of Directory Services Using the X.500 Protocol** Versione 1992, stato: marzo 1992 Fonte: https://tools.ietf.org/pdf/rfc1309.pdf
[9]	**IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework** Versione 2003, stato: novembre 2003 Fonte: https://tools.ietf.org/pdf/rfc3647.pdf
[10]	**RFC 2459: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile** Versione 1999, stato gennaio 1999 Fonte: https://tools.ietf.org/pdf/rfc2459.pdf
[11]	**RFC 2510, Internet X.509 Public Key Infrastructure – Certificate Management Protocols** Versione 1999, stato marzo 1999 Fonte: https://tools.ietf.org/pdf/rfc2510.pdf
[12]	**FIPS 140-2: Requisiti di sicurezza per i moduli crittografici, National Institute of Standards and Technology, Federal Information Processing Standards** Versione 1994
[13]	**Electronic Signatures an Trust Infrastructures (ESI); Cryptographic Suites ETSI TS 11 312 V1.5.1 (2024-12)**
[14]	**Swiss Government SSCD Evaluation Criteria**
[15]	**Swiss Government SSCD Protection Profile**

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 A – qualificati per le persone fisiche e dei certificati amministrativi per le persone giuridiche nell'ambito della Swiss Government PKI (di seguito "SG-PKI").

Destinatari

Il documento si rivolge principalmente ai LRA-Officer qualificati per il rilascio di certificati di classe A degli uffici pubblici e le aziende collegate allo Stato.

Termini e abbreviazioni utilizzati

Le abbreviazioni e i termini specifici 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 segno di riconoscimento posto tra parentesi quadre, ad esempio [1]. Nella tabella «Documenti di riferimento» sono indicati i rimandi con un segno distintivo posto tra parentesi quadre.

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 IV - CP_CPS EN» (di seguito «CP/CPS») [1] è il dispositivo normativo determinante per i certificati qualificati di classe A e di certificati regolamentati della SG-PKI. Lo scopo del documento è definire i requisiti del CP/CPS per le persone della SG-PKI competenti del rilascio.

1.2 Campo di applicazione

La presente direttiva si applica a tutti i collaboratori che operano nell'ambito della LRA dei certificati qualificati e regolamentati di classe A. La SG-PKI può delegare i compiti della LRA della classe A ad altre unità organizzative che designeranno a loro volta i collaboratori esecutivi. Le attività relative ai certificati amministrativi regolamentati non possono essere delegate ad altre unità organizzative.

Nel rilascio dei certificati qualificati e regolamentati di classe A si applica esclusivamente:

- la procedura di rilascio con l'identificazione del richiedente.

1.3 SG-PKI – certificati qualificati e regolamentati di classe A

Un certificato di firma qualificato o il certificato ufficiale regolamentato viene rilasciato su un modulo di sicurezza hardware (HSM). L'accesso alla chiave privata per la firma qualificata viene attivato tramite il certificato di autenticazione di classe B oppure il MobileID, nel caso del certificato ufficiale regolamentato, tramite l'applicazione specialistica registrata presso il servizio di firma.

2 Profilo dei requisiti del LRA-Officer e rispettivi compiti

2.1 Profilo dei requisiti 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, ad esempio a un controllo di sicurezza di base OCSP (Ref. **Fehler! Verweisquelle konnte nicht gefunden werden.**)**Fehler! Verweisquelle konnte nicht gefunden werden.** (v. n. 3.7);
- divieto di inserire dati nell'Admin-Directory e di modificare quelli esistenti;
- Per certificati qualificati: esperienza pregressa di almeno 6 mesi in qualità di LRA-Officer per certificati di classe B;
- Per certificati regolamentati: Solo collaboratori della SG-PKI, che hanno seguito un corso di formazione interno

2.2 Compiti del LRA-Officer

Il LRA-Officer ha i seguenti compiti:

- ✓ identificare il richiedente;
- ✓ verificare i dati nell'Admin-Directory;
- ✓ rilasciare i certificati;
- ✓ revocare i certificati;
- ✓ informare i clienti riguardo a:
  - i dati di attivazione,
  - la protezione dei dati di attivazione,
  - i loro diritti e obblighi,
  - le «Condizioni contrattuali e di utilizzo per i certificati qualificati di classe A» [5],
- ✓ compilare le liste di controllo;
- ✓ tenere un registro di tutte le attività che riguardano i certificati;
- ✓ gestire e conservare i dossier dei titolari dei certificati;
- ✓ Tenersi aggiornati in modo proattivo sulle normative, sui processi e sugli strumenti tecnici relativi ai certificati regolamentati rilasciati dalle autorità

2.3 Responsabilità

Il LRA-Officer è consapevole di non poter trasmettere alcuna richiesta alla SG-PKI qualora l'identificazione del richiedente non possa essere effettuata in modo corretto o completo.

La violazione di tale obbligo può comportare la revoca immediata dell'autorizzazione LRAO nonché, se necessario, ulteriori provvedimenti legali.

Il LRA-Officer è responsabile di tutti i richiedenti da lui identificati. È responsabile per i danni e le conseguenze derivanti da un'identificazione errata o insufficiente.

2.4 Obbligo di segnalazione

Eventuali cambiamenti organizzativi, cambiamenti di nome (ad esempio in seguito a matrimonio) o modifiche all'indirizzo e-mail del responsabile LRA devono essere comunicati immediatamente alla SG-PKI.

3 Aspetti operativi generali

3.1 Orari di servizio della LRA

Gli orari di servizio della LRA vengono stabiliti dalle unità organizzative responsabili.
Gli orari di servizio dell'UFIT sono indicati nelle rispettive schede informative disponibili sul portale clienti online dell'UFIT.

3.2 Supporto della LRA

A supporto della LRA può intervenire il gruppo 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 gruppo operativo può essere contattato tramite il Service Desk UFIT (tel. 058 465 88 88).

Per domande e comunicazioni urgenti riguardanti la sicurezza, tramite il Service Desk UFIT (tel. 058 465 88 88) è possibile contattare anche il responsabile della sicurezza della SG-PKI (tel. 058 465 88 88).

Per questioni e comunicazioni meno urgenti riguardanti la sicurezza è possibile inviare un'e-mail all'indirizzo pki-secoff@bit.admin.ch . Gli ordini e le domande di carattere generale possono essere inviati per e-mail all'indirizzo signaturservice@bit.admin.ch .

3.3 Moduli e dati dei clienti

È obbligatorio utilizzare i moduli specificati nelle presenti direttive ed emessi dalla SG-PKI è obbligatorio, salvo quando si fa espressamente riferimento ad alternative consentite (in formato cartaceo o elettronico). Per motivi di tracciabilità non è ammesso l'utilizzo di moduli diversi o di soluzioni elettroniche.

I dossier dei clienti (moduli di richiesta procura per certificati regolamentati, condizioni di utilizzo firmate, richieste di revoca ecc.) devono essere conservati sottochiave (principio «clear desk»); la porta del locale deve essere chiusa a chiave o i documenti devono essere riposti in un armadio chiuso a chiave.

I dossier dei clienti salvati in un archivio elettronico devono essere accessibili soltanto alle persone autorizzate, ossia ai LRA-Officer e agli ispettori. Inoltre, deve essere garantito il rispetto delle condizioni per i termini di conservazione di cui al numero 3.5. Tutti i documenti archiviati devono essere disponibili in formato PDF/A e muniti di una firma valida.

3.4 Registro

Nel registro vengono annotate tutte le attività della LRA riguardanti il rilascio e la revoca dei certificati oppure altri eventi importanti, ad esempio:

- il rilascio di certificati;
- la revoca di certificati;

Il LRA-Officer può decidere di tenere i registri in formato cartaceo (v. modello «Registro della LRA della Swiss Government PKI per certificati qualificati di classe A per persone fisiche secondo la FiEle ») o elettronico. In quest'ultimo caso il LRA-Officer deve stampare, firmare e archiviare i re-

gistri 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 sia garantita la cronologia.

I dati del registro devono essere o conservati secondo i termini di archiviazione al capitolo 3.5 – *Termini die conservazione*

Nel registro devono essere annotate almeno le informazioni seguenti:

1. il numero progressivo della registrazione (N.B.: la cronologia deve essere tracciabile. È consentito cioè ricominciare ogni anno una nuova numerazione se ad esempio si antepone l'anno);
2. la data;
3. il LRA-Officer che si occupa dell'esecuzione;
4. il nome del richiedente;
5. il tipo di attività (RI: rilascio, RE: revoca);
6. il visto o la firma elettronica provvista di marca temporale del LRA-Officer.
7. Nel caso di certificati regolamentati: CN del certificato regolamentato

3.5 Termini di conservazione

I moduli, i dati dei clienti, i moduli e i registri di cui ai numeri 3.3 e 3.4 devono essere conservati ed essere a disposizione degli ispettori per almeno 11 anni a partire dalla scadenza della validità del rispettivo certificato.

3.6 Smaltimento

I documenti cartacei non più necessari riguardanti la LRA (direttive, liste di controllo, appunti, copie ecc.) o i clienti (richieste, elenchi ecc.) devono essere distrutti con un tritacarte o gettati in un contenitore di sicurezza per poi essere smaltiti

3.7 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:

- eseguire un controllo di sicurezza di base OCSP presso il servizio specializzato CSP del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS)

e/o

- adottare misure proprie per verificare l'affidabilità del candidato, ad esempio:
  - ✓ il controllo dell'identità (passaporto o carta d'identità),
  - ✓ la verifica di referenze professionali e private,
  - ✓ la verifica della completezza e della coerenza del curriculum vitae,
  - ✓ il controllo delle qualifiche accademiche e professionali dichiarate,
  - ✓ la verifica degli estratti dal registro delle esecuzioni e dal casellario giudiziale.

Il funzionario avente diritto di firma dell'autorità conferma alla SG-PKI l'affidabilità del candidato conformemente già menzionata alla raccomandazione o di aver effettuato la verifica in modo analogo. A verifica ultimata, il funzionario giudica il candidato affidabile e integro e accerta la presenza delle competenze necessarie per l'esercizio del ruolo di LRA-Officer, sensibile sotto il profilo della sicurezza.

I collaboratori della SG-PKI vengono sottoposti a un controllo di sicurezza di base secondo il OCSP.

3.8 Confidenzialità e protezione dei dati

I LRA-Officer devono firmare una dichiarazione di confidenzialità, che è parte integrante del modulo di richiesta.

I LRA-Officer e i loro clienti devono osservare imperativamente la legislazione sulla protezione dei dati.

Le informazioni che riguardano i clienti o i dati importanti della LRA o della CA devono essere trasmessi in forma crittografata.

3.9 Formazione del personale

Tutti LRA-Officer devono assolvere una formazione e superare un esame scritto. Per essere ammessi alla formazione è necessaria un'esperienza pregressa di almeno sei mesi in qualità di LRA-Officer per certificati di classe B. Al termine della formazione i partecipanti devono dimostrare di possedere le conoscenze e le competenze sufficienti per operare come LRA-Officer per certificati di classe A.

Se un richiedente non soddisfa le condizioni previste nella procedura di certificazione o è stato bocciato all'esame, non può svolgere nemmeno la funzione di sostituto. Può però frequentare di nuovo il corso e ripetere l'esame.

Se un LRA-Officer riscontri alcune 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 ricercare una soluzione insieme a quest'ultima.

Il rilascio dei certificati regolamentati viene gestito internamente (SG-PKI).

In caso di violazione delle direttive per la registrazione, la SG-PKI può sottrarre la qualificazione del LRA-Officer.

3.10 Formazione continua / Aggiornamento della formazione

Il LRA-Officer deve tenersi sempre aggiornato, in particolare su questi documenti di riferimento: «CP/CPS» [1], le direttive per la registrazione (presente documento), le «Condizioni contrattuali e di utilizzo per i certificati qualificati di classe A» [5]. A tal fine la SG-PKI mette a disposizione le informazioni e la documentazione aggiornata nell'area riservata ai clienti sulla pagina Internet http://www.pki.admin.ch. Inoltre, la SG-PKI si impegna a notificare per e-mail eventuali modifiche importanti. A sua volta, il LRA-Officer che riceve un'e-mail da parte della SG-PKI è tenuto a leggere le informazioni al riguardo pubblicate nell'area riservata ai clienti sulla pagina Internet della SG-PKI.

La SG-PKI propone regolarmente corsi di formazione continua specifici, a cui i LRA-Officer possono essere obbligati a partecipare.

Se un LRA-Officer riscontri alcune 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 ricercare una soluzione insieme a quest'ultima.

4 Verifica di conformità

La SG-PKI è tenuta a verificare l'attuazione del CP/CPS ogni 18 mesi. In particolare, deve verificare l'osservanza delle presenti direttive da parte dei LRA-Officer. La verifica di conformità può essere effettuata direttamente dalla SG-PKI o da un organo esterno da essa incaricato.

In caso di mancato superamento della verifica di conformità il LRA-Officer può perdere la qualifica. Se vengono rilevate lacune gravi, il responsabile SG-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 qualificati di classe A

5.1 Panoramica

Ai certificati qualificati di classe A per persone fisiche e di classe A certificati regolamentati per persone giuridiche si applica un'unica procedura:

Classe A – certificati qualificati per persone fisiche
Viene fornita una coppia di chiavi (firma)
Non è possibile concedere sospensioni
Persone fisiche: Non è possibile concedere procure Persone giuridiche: È possibile concedere procure
Il recupero della chiave (Key Recovery) non è possibile
Non è possibile il rinnovo del certificato (Renewal)

Tabella 1: Procedura per certificati qualificati – persone fisiche e certificati regolamentati per le persone giuridiche

5.2 Procedura di rilascio di un certificato

Qui di seguito le fasi salienti della procedura di rilascio:

Procedura
Spetta esclusivamente al LRA-Officer classe A a effettuare l'identificazione personale del richiedente.
In caso di certificato regolamento: verifica preventiva della domanda presentata, comprese la procura richiesta e l'iscrizione nel registro UID.
Il LRA-Officer verifica l'iscrizione del richiedente nell'Admin-Directory.
Il LRA-Officer fornisce al richiedente le istruzioni sui dati di attivazione e sulla loro protezione.
Il LRA-Officer crea una richiesta per il partecipante

Tabella 2: procedura di rilascio

5.2.1 Unità autorizzate a richiedere un certificato

Persona fisica:
La decisione relativa al rilascio di certificati qualificati spetta alle rispettive unità organizzative.

Persona giuridica:
Il presupposto fondamentale per ottenere un certificato ufficiale regolamentato è che l'organizzazione sia un'unità UID ai sensi dell'articolo 3 capoverso 1 lettera c della legge federale del 18 giugno 2014 sul numero di identificazione delle imprese (LUI). Il richiedente deve essere autorizzato a firmare per la rispettiva unità UID. Deve poter dimostrare tale autorizzazione mediante un estratto autenticato del registro di commercio o una procura firmata in modo giuridicamente valido.

5.2.2 Procedura per la richiesta di un certificato

La richiesta di certificati qualificati e regolamentati avviene tramite Digital Workplace (DWP). L'ordine deve essere tracciabile. La SG-PKI mette a disposizione un modulo che contiene tutti i

dati necessari per la richiesta conformemente all'articolo 7 capoverso 3 lettera a FiEle e all'articolo 5 OFiEle (v. [2][3]).

5.2.3 Rilascio

Il LRA-Officer procede secondo l'attuale lista di controllo Walktrough e lista di controllo per il rilascio di certificati qualificati a persone fisiche. La lista di controllo fa parte della documentazione relativa al rilascio e deve essere compilata, firmata digitalmente e archiviata.

5.2.3.1 Verifica dell'iscrizione nell'Admin-Directory

Per ricevere un certificato, è indispensabile che il richiedente sia registrato nell'Admin-Directory. Al proposito devono essere soddisfatte le seguenti condizioni:

1. nel campo «E-Mail» deve figurare un indirizzo di posta elettronica completo e plausibile. Oltre a fissare un appuntamento per il rilascio del certificato, ciò consente anche di verificare l'indirizzo di posta elettronica del richiedente (punto 2 della lista di controllo);
2. se è presente più di un'iscrizione: l'iscrizione che serve per il rilascio del certificato deve poter essere identificata in maniera univoca tramite il suffisso del nome.

Se l'iscrizione del richiedente nell'Admin-Directory è errata o non è presente, occorre inviare una notifica nel sistema dei dati del personale del proprio ufficio. Si riprenderà la procedura di rilascio soltanto a correzione avvenuta nell'Admin-Directory.

5.2.3.2 Iscrizione nel registro pubblico (persone giuridica)

Il presupposto per il rilascio dei certificati è che l'autorità indicata nella domanda esista come persona giuridica e sia iscritta nel registro pubblico UID (www.uid.admin.ch).

Se l'autorità non è iscritta o non è correttamente iscritta in un registro pubblico, essa deve provvedere alla creazione dell'iscrizione o alla sua correzione. La denominazione massima dell'autorità non deve superare i 64 caratteri. Se nel registro non tutti i dati rilevanti sono accessibili al pubblico, il richiedente deve allegare una copia autenticata di tutti i dati essenziali richiesti. La procedura può proseguire solo quando tutti i documenti e le registrazioni sono presenti in modo corretto e completo.

5.2.3.3 Verifica del modulo di richiesta

Verificare la completezza e la correttezza del modulo di richiesta.

1. Il richiedente è autorizzato secondo il numero 5.2.1 a presentare una domanda a questo LRA-Officer?
2. I dati del richiedente indicati sul modulo corrispondono a quelli iscritti nell'Admin-Directory?
3. Il modulo è compilato integralmente? La data indicata è corretta? La firma è valida?

Inoltre, nel caso di persone giuridiche

4. È presente l'iscrizione nel registro UID. (Estratto del registro UID. Qualora nel registro UID non fossero pubblicati tutti i dati relativi alle caratteristiche principali, occorre allegare l'estratto autenticato più recente)
5. È presente una procura o un'autorizzazione alla firma per il rilascio del certificato (estratto autenticato del registro delle imprese o delega di rappresentanza debitamente firmata)

5.2.3.4 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 munirsi di un documento d'identità valido. Alla data della registrazione il documento d'identità non deve risultare scaduto;
3. fornirgli i dati di contatto del LRA-Officer in caso di domande o per convenire una data diversa da quella proposta.

5.2.3.5 Verifica dell'identità del richiedente

Il richiedente deve presentarsi personalmente dal LRA-Officer. L'identità del richiedente deve essere verificata sulla base di un documento di viaggio (passaporto o una carta d'identità) rilasciato dalla Svizzera oppure riconosciuto per l'entrata in Svizzera. La carta di legittimazione o la patente di guida non sono accettate ai fini dell'identificazione. La verifica dell'identità del richiedente comprende i due elementi seguenti:

1. la verifica dell'autenticità del documento di viaggio presentato. A tal fine devono essere osservati i seguenti punti:
    a. validità (al momento della registrazione il documento non deve essere scaduto),
    b. presenza delle caratteristiche di sicurezza note: devono essere verificate almeno quattro caratteristiche di sicurezza ufficiali del documento. In caso di dubbi, occorre coinvolgere una persona in possesso di solide conoscenze in materia,
    c. corrispondenza tra i dati indicati nel documento di viaggio e quelli indicati nella richiesta,
    d. corrispondenza tra la firma apposta nel documento di viaggio e quella apposta nel modulo di richiesta;
2. l'identificazione personale: verificare la corrispondenza tra la persona e la sua foto riportata nel documento di viaggio.
3. Verifica della procura: occorre verificare i certificati di procura.

5.2.3.6 Informazioni sui diritti e doveri del richiedente

Il richiedente deve essere informato verbalmente dei propri diritti e doveri. In tale occasione, gli vengono illustrate verbalmente le «*Condizioni d'uso e di utilizzo Classe A – Certificati regolamentati e qualificati ai sensi della FiEle*».

Il LRA-Officer decide se il richiedente dispone delle conoscenze di base necessarie per un uso appropriato della chiave di firma privata e del certificato e se è a conoscenza dei propri diritti e doveri. Se il richiedente dà motivo di ritenere che non sia in grado o non intenda esercitare i propri diritti e doveri, il funzionario LRA nega il completamento della procedura.

5.2.3.7 Preparare l'emissione sul servizio di firma

Il LRA-Officer registra i dati nell'interfaccia utente amministrativa del servizio di firma sulla base della domanda verificata. Una volta registrati tutti i dati, è possibile generare il CSR.

5.2.3.8 Richiesta di certificati

La richiesta del certificato viene effettuata dal LRA-Officer con l'ausilio dello strumento CRW. Dopo avere effettuato il login, il LRA-Officer sceglie la policy per il certificato qualificato o il certificato regolamentato di classe A.

5.2.3.9 DN del certificato regolamentato

Il DN del certificato di autorità certificato va inserito secondo le seguenti regole:

Nome distinto del certificato		
C	CH o LI: codice paese secondo la norma ISO 3166-1. Indica il paese dell'autorità indicata con l'RDN «O»	obbligatorio
O	La chiave O deve corrispondere al nome presente nel registro UID (deve essere verificata dal CSP, max. 64 caratteri)	obbligatorio
CN	Denominazione comunemente utilizzata dell'ente amministrativo. Il nome non deve necessariamente corrispondere esattamente al nome registrato (denominazione secondo il registro UID)	obbligatorio
OI[1]	Numero UID dell'autorità emittente (secondo il registro UID), come richiesto dalla FiEle	obbligatorio
OU_{1-2}	Denominazione dettagliata dell'unità organizzativa (dipartimento, sezione, ecc.) associata al certificato. È possibile specificare due campi OU	opzionale
OU_3	Identificazione delle autorità: GE - 0220 – Abbreviazione o denominazione dell'ente: Autorità federale (Ufficio federale) GE - 0221 - Codice cantonale - Codice o denominazione dell'ufficio dell'autorità cantonale GE - 0222 - Codice cantonale - Codice storico BFSNR - Codice o denominazione dell'ufficio di un distretto GE - 0223 - Storia BFSNR - Sigla o denominazione dell'autorità comunale	obbligatorio
L	Nome del comune in cui ha sede l'ente	opzionale
SP	Denominazione del cantone in cui ha sede l'autorità	opzionale
E-Mail	Indirizzo e-mail del certificato (ad es.: «info@uffico.admin.ch») In caso di verifica automatica di un documento firmato elettronicamente, può essere riportato in un rapporto di verifica per indicare l'ente di riferimento per quel tipo di documento firmato	opzionale

5.2.3.10 Emissione del certificato

Nel sistema AIS viene generato il CSR, che viene poi firmato tramite il CRW, dove viene emesso il certificato. Successivamente, il certificato può essere scaricato e caricato nell'interfaccia utente amministrativa del server di firma.

5.2.3.11 Tenuta del registro e firma della lista di controllo

Il LRA-Officer deve annotare le attività svolte nel registro della LRA attenendosi alle regole di cui al numero 3.4Egli deve dapprima verificare se la lista di controllo è completa e poi apporvi la firma.

5.2.3.12 Archiviazione del dossier del cliente

La richiesta compilata incluso le condizioni contrattuali e di utilizzo per i certificati qualificati die classe A, la lista di controllo firmata nonché gli ulteriori documenti giustificativi relativi al certificato regolamentato per autorità vengono archiviati nel dossier per clienti.

5.3 Procedura di revoca di un certificato

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 delle RU (Servizio del personale);
- i superiori diretti;
- il responsabile della SG-PKI;
- il responsabile della sicurezza della SG-PKI;
- il LRA-Officer competente;
- l'incaricato della sicurezza informatica dell'unità amministrativa.
- Inoltre, per il certificato delle autorità: persone autorizzate a firmare secondo quanto riportato nell'UID o nel registro di commercio

5.3.2 Modalità di richiesta di una revoca

La revoca può essere richiesta in qualsiasi momento dalle persone menzionate al capitolo 5.3.1 inviando un modulo firmato via e-mail alla SG-PKI.

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

5.3.3 Motivi di revoca

I motivi che portano a una revoca sono i seguenti:

- la smartcard è stata rubata o è andata persa;
- la smartcard è difettosa;
- il titolare del certificato ha dimenticato il PIN e il PUK;
- cessazione del rapporto di lavoro;
- i dati contenuti nel certificato sono cambiati (nome, indirizzo di posta elettronica, nome dell'ente, ecc.);
- 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);
- riorganizzazione
- il titolare del certificato/utenti attuali autorizzati non osserva le direttive del CP/CPS o le condizioni di utilizzo;
- il LRA-Officer ritiene opportuna una revoca per altri motivi.

5.3.4 Procedura

Una domanda di revoca deve essere trattata sempre immediatamente. In caso di dubbi riguardo alla validità di una richiesta di revoca (ad es. se viene presentata per telefono) è bene ricordarsi che lo scopo per cui viene revocato un certificato è tutelare il cliente da possibili danni derivanti dall'utilizzo illecito del suo certificato. 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 seguenti:

- 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?
- L'ente richiedente è competente per il certificato di autorità pubblica ed è autorizzato a presentare la richiesta di revoca?

5.3.4.2 Compilazione del modulo di revoca

Poiché per i certificati di classe A la revoca deve essere effettuata nell'applicazione della LRA, i motivi di revoca devono essere documentati nell'apposito modulo. Se il modulo non è stato compilato dal richiedente, vi provvede il LRA-Officer e lo archivia nel dossier del cliente.

5.3.4.3 Revoca

Persona fisica

Anzitutto si avvia una ricerca del titolare del certificato nell'applicazione della LRA.

Persona giuridica

Per la revoca, il certificato viene cercato nell'applicazione LRA in base al CN (Common Name) o all'indirizzo e-mail e al numero di serie.

Poi si seleziona il certificato in questione e si attua la revoca. Il titolare del certificato riceve automaticamente all'indirizzo e-mail indicato nel certificato una conferma a operazione conclusa.

5.3.4.4 Chiusura amministrativa della procedura

Il modulo di revoca, in originale o in copia, è archiviato nel dossier del cliente. La procedura di revoca è documentata nel registro come previsto al numero 3.4.

6 Moduli e liste di controllo

Per le procedure descritte in precedenza sono disponibili le liste di controllo e i moduli indicati di seguito, tutti ottenibili singolarmente presso il responsabile SG-PKI.

6.1 Modulo di richiesta di un certificato

I clienti possono decidere liberamente se predisporre un modulo ad hoc specifico per la propria organizzazione, che deve contenere almeno i dati seguenti:

- cognome e nome;
- unità organizzativa;
- tipo di documento d'identità (passaporto o carta d'identità);
- numero del documento d'identità;
- indirizzo di posta elettronica;
- luogo d'origine;
- data di nascita.

Il cliente firma il modulo di richiesta e conferma che le informazioni ivi contenute sono corrette, nonché il rispetto delle condizioni d'uso. Il modulo è parte integrante della documentazione relativa alla procedura di rilascio.

Gli uffici che usufruiscono dei servizi di supporto dell'UFIT possono ordinare il certificato di classe A per persone fisiche anche mediante DWP.

6.2 Condizioni contrattuali e di utilizzo per i certificati qualificati di classe A

Le «Condizioni contrattuali e di utilizzo per i certificati qualificati di classe A»[5], redatte appositamente per gli utenti finali, contengono le informazioni fondamentali. Questo documento è parte integrante della documentazione relativa alla procedura di rilascio rilevante ai fini delle verifiche. Le informazioni complete sono contenute nel documento «Swiss Government PKI - Root CA IV - CP_CPS EN» [1].

6.3 Modulo di revoca

Se il «Modulo per la revoca di certificati qualificati per persone fisiche» non è stato compilato dal richiedente, deve provvedervi il LRA-Officer e apporvi la firma. Il modulo è parte integrante della documentazione relativa alla procedura di rilascio rilevante ai fini delle verifiche.

Se viene richiesta la revoca di un certificato di firma qualificato utilizzato con il servizio di firma, sia il certificato di firma qualificato che il materiale chiave associato devono essere cancellati dall'HSM del servizio di firma. Per questo processo viene fornita una lista di controllo corrispondente.

6.4 Rilascio del certificato e lista di controllo

Il documento «rilascio di certificati qualificati per persone fisiche e lista di controllo» funge da ausilio per il LRA-Officer nella procedura di rilascio. Esso deve essere compilato e archiviato.

6.5 Registro

Il registro è parte integrante della documentazione relativa alla procedura di rilascio rilevante ai fini delle verifiche. Esso riporta tutte le attività del LRA-Officer concernenti i certificati di classe A per persone fisiche.

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 della sicurezza PKI dell'UFIT.

8 Proposte di modifica

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

Responsabile servizio SG-PKI
Ufficio federale dell'informatica e della telecomunicazione UFIT
Campus Meielen
Eichenweg 3
CH-3003 Berna

E-Mail: pki-secoff@bit.admin.ch