



Condizioni contrattuali e di utilizzo per i certificati di classe A – Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)

V2.5, 02.03.2026

Nel suo ruolo di Trust Service Provider (TSP), la Swiss Government PKI (SG-PKI) dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) gestisce, su incarico del settore Trasformazione digitale e governance delle TIC (TDT), le infrastrutture a chiave pubblica (Public Key Infrastructure, PKI) delle autorità federali della Confederazione Svizzera. I certificati di classe A per la firma elettronica regolamentata o qualificata secondo la legge sulla firma elettronica (FiEle; di seguito «certificati») 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 di questi certificati della SG-PKI sottostanno alle disposizioni del presente documento. Ogni anno la SG-PKI verifica le disposizioni e, laddove necessario, le adegua alle prescrizioni legali vigenti e ai requisiti normativi definiti per le infrastrutture a chiave pubblica. La versione in vigore del presente documento è pubblicata sul sito Internetⁱ della SG-PKI. I titolari dei certificati vengono informati per e-mail in merito alla pubblicazione della versione aggiornata del documento. Trascorsi 30 giorni dall'invio di tale comunicazione, la nuova versione si considera tacitamente accettata, a meno che durante questo lasso di tempo non venga disposta la revoca immediata del certificato.

Indice

1 Esattezza delle informazioni	2
2 Protezione della chiave privata e del certificato	2
3 Ricevimento del certificato	3
4 Utilizzo del certificato	3
4.1 Disponibilità	5
5 Comunicazione e revoca	5
6 Cessazione dell'utilizzo del certificato	6
7 Responsabilità	6
8 Basi giuridiche, validità dei documenti ed elementi del contratto	7
8.1 Foro competente e diritto applicabile	7
8.2 Reclami e controversie	7
8.3 Verifica della conformità con CP/CPS	8
9 Contenuto e validità dei certificati regolamentati e qualificati di classe A	8
10 Informazioni per «relying parties»	9
11 Richiesta e ottenimento di certificati di classe A	9
12 Conservazione dei registri («event log»)	10
13 Dichiarazione di riconoscimento e di consenso	10
14 Contatti del TSP	10

1 Esattezza delle informazioni

La persona fisica o giuridica¹ titolare di un certificato di classe A della SG-PKI (di seguito «titolare²») si impegna a fornire al TSP informazioni esatte ed esaustive necessarie per la procedura di rilascio e l'elaborazione del contenuto del certificato. Durante la procedura di rilascio dei certificati vengono impiegati complessi meccanismi di verifica e sicurezza, che consentono di stabilire l'identità del richiedente³ con un elevato grado di sicurezza. Ad esempio, prima del rilascio del certificato, il richiedente deve presentarsi di persona ed essere identificato sulla base di un documento di viaggio valido. Il certificato è indissolubilmente legato al titolare.

- Certificati per persone fisiche

Nome(i), cognome(i), suffisso (l'iscrizione nell'Admin-Directory della Confederazione) e indirizzo e-mail del titolare vengono sempre indicati nel certificato. Presso la SG-PKI vengono registrati e archiviati altri dati personali, quali la data di nascita e la copia scansionata di un documento di viaggio valido.

- Certificati per persone giuridiche

Il richiedente deve essere autorizzato a rappresentare il titolare. L'attestazione di procura scritta e la copia scansionata di un documento di viaggio valido del richiedente vengono registrati e archiviati presso la SG-PKI.

Nel certificato il titolare è indicato con un «Distinguished Name» secondo lo standard X.509. Il certificato contiene l'IDI e i nomi ufficiali della persona giuridica (ad es. autorità) negli attributi corrispondenti «Organizzazione» e «ID dell'organizzazione».

Il titolare è tenuto a informare immediatamente il TSP in caso di modifica dei dati contenuti nel certificato.

2 Protezione della chiave privata e del certificato

La chiave privata del certificato di classe A è salvata su una memoria centrale altamente sicura (HSM, servizio di firma) della SG-PKI.

- Servizio di firma dell'UFIT

Per attivare la chiave privata necessaria per la creazione di una firma/sigillo elettronico regolamentato, l'utente deve utilizzare, nell'apposita applicazione, il certificato di autenticazione memorizzato sulla smart card personale di classe B con il relativo PIN o il MobileID personale. Se il servizio di firma viene utilizzato in un'applicazione specifica dove, per attivare la chiave necessaria per la creazione di una firma elettronica viene utilizzata una chiave comune memorizzata nell'applicazione, va dimostrato che la chiave e i dati di accesso siano conservati in modo sicuro. In caso di utilizzo di MobileID, le condizioni d'usoⁱⁱ separate di MobileID sono parte integrante del presente documento.

Il titolare si impegna a prendere tutte le misure necessarie a garantire il controllo, la confidenzialità e la protezione contro la perdita e l'utilizzo illecito della chiave privata e degli eventuali dati di accesso ad essa associati. Le chiavi private dei certificati possono e devono essere utilizzate soltanto in combinazione con i certificati stessi e soltanto per lo scopo (firma) stabilito nei certificati.

Le chiavi private dei certificati per persone fisiche non sono trasferibili e per nessun motivo possono essere rese accessibili a terzi.

¹ Secondo la FiEle i certificati regolamentati possono essere rilasciati a persone fisiche e unità IDI. La SG-PKI rilascia i certificati regolamentati unicamente a persone giuridiche iscritte nel registro IDI. Alle persone fisiche la SG-PKI rilascia certificati qualificati.

² Il termine «titolare» indica la persona fisica o giuridica a cui è stato rilasciato il certificato. Una persona giuridica può essere, ad esempio, un'autorità.

³ Il termine «richiedente» indica la persona fisica che richiede il certificato per se stessa o per la persona giuridica da essa rappresentata in virtù di un potere di rappresentanza.

Il titolare risponde di qualsiasi danno causato dalla trasmissione a terzi della chiave privata, dei dati di accesso alla chiave o di eventuali dati di attivazione o smart card ad essi associati.

Gli HSM utilizzati soddisfano i requisiti della FiEle.

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

3 Ricevimento del certificato

Il titolare verifica il contenuto del certificato al momento del suo ricevimento e si assicura, per tutta la durata del certificato, che le informazioni ivi contenute siano corrette.

4 Utilizzo del certificato

- Certificati qualificati per persone fisiche

I certificati qualificati di classe A per persone fisiche vengono utilizzati esclusivamente per la firma elettronica attendibile e giuridicamente valida di documenti, equiparata alla firma autografa. Essi confermano l'autenticità e l'integrità dei documenti, come pure l'accettazione da parte del firmatario del relativo contenuto. Il titolare garantisce di conoscere il contenuto, lo scopo e le conseguenze dell'utilizzo del certificato. Inoltre, si impegna a utilizzare il certificato e la relativa chiave privata nel rispetto delle prescrizioni legali vigenti come pure delle disposizioni del presente documento e in conformità con le direttive della sua Unità amministrativa di competenza o del suo datore di lavoro.

I certificati qualificati di classe A servono esclusivamente allo scopo succitato e non forniscono informazioni né garanzie aggiuntive. In particolare, tali certificati non garantiscono che il titolare stia utilizzando il certificato correttamente e legalmente.

Inoltre, i certificati qualificati di classe A non garantiscono che il titolare indicato nel certificato:

- sia effettivamente coinvolto nelle attività aziendali;
- si attenga alle prescrizioni legali;
- sia affidabile e agisca con serietà nel contesto lavorativo; o
- possieda le competenze professionali, tecniche, organizzative o di altro genere per utilizzarlo correttamente.

Al momento del rilascio di un certificato qualificato di classe A, la SG-PKI verifica i punti elencati di seguito:

- **esistenza giuridicamente valida:** il titolare indicato nel certificato esiste come persona fisica o giuridica;
- **identità:** il nome del titolare indicato nel certificato (escluso il suffisso) corrisponde a quello indicato nel suo documento di viaggio valido;
- **autorizzazione:** la SG-PKI ha intrapreso tutti i passi necessari e ragionevolmente esigibili per verificare che il titolare indicato nel certificato sia autorizzato a ottenerlo;
- **esattezza dei dati:** la SG-PKI ha intrapreso tutti i passi necessari e ragionevolmente esigibili per garantire che le informazioni e i dati contenuti nel certificato siano esatti
stato: la SG-PKI rende disponibili online 7 giorni su 7, 24 ore su 24 lo stato del certificato e le informazioni relative alla sua validità e revoca conformemente alle disposizioni legali;
- **condizioni di utilizzo:** il richiedente è stato informato dal LRA-Officer (Local Registration Authority Officer) in merito ai diritti e agli obblighi descritti nel presente documento. Il LRA-Officer della SG-PKI ha risposto in modo chiaro alle domande del

richiedente a tale proposito. Il richiedente ha letto il documento, ne ha preso atto e lo ha firmato;

- revoca: se del caso, la SG-PKI può revocare immediatamente il certificato in presenza di uno dei motivi citati nel presente documento.

- **Certificati regolamentati per persone giuridiche**

I certificati regolamentati di classe A per persone giuridiche, spesso denominati anche «certificati per le autorità», sottostanno alle disposizioni della FiEle, dell'ordinanza sulla firma elettronica (OFiEle) e ad altre disposizioni legali. Possono essere utilizzati esclusivamente per la firma di documenti elettronici.

La firma mediante un certificato regolamentato di classe A per persone giuridiche genera un sigillo elettronico. Le unità amministrative e le autorità possono firmare elettronicamente i documenti ufficiali mediante un certificato rilasciato per l'ufficio corrispondente e una marca temporale elettronica qualificata (art. 2 lett. j FiEle). I cittadini e le imprese devono avere la possibilità di verificare i documenti ufficiali firmati elettronicamente (tramite sigilli elettronici) dalle autorità al fine di garantire che essi provengano effettivamente dall'autorità competente. Inoltre, la marca temporale elettronica qualificata che viene aggiunta permette di determinare il momento preciso in cui la firma è stata apposta.

I certificati regolamentati di classe A servono esclusivamente allo scopo succitato e non forniscono informazioni né garanzie aggiuntive. In particolare, non garantiscono che la persona fisica stia utilizzando il certificato correttamente e legalmente.

Inoltre, i certificati regolamentati di classe A non garantiscono che l'utente:

- sia effettivamente coinvolto nelle attività aziendali;
- si attenga alle prescrizioni legali;
- sia affidabile e agisca con serietà nel contesto lavorativo;
- possieda le competenze professionali, tecniche, organizzative o di altro genere per utilizzarlo correttamente.

Al momento del rilascio di un certificato regolamentato di classe A, la SG-PKI verifica i punti elencati di seguito:

- **esistenza giuridicamente valida:** la persona giuridica indicata nel certificato regolamentato esiste ed è iscritta nel registro pubblico IDIⁱⁱⁱ.
- **identità:** il nome indicato nel certificato regolamentato nell'attributo «O=» corrisponde al nome della persona giuridica iscritta nel registro IDI;
- **autorizzazione:** la SG-PKI ha intrapreso tutti i passi necessari e richiesti dalla legge (FiEle) per accertare che il richiedente del certificato sia autorizzato a ottenerlo;
- **esattezza dei dati:** la SG-PKI ha intrapreso tutti i passi necessari e ragionevolmente esigibili per garantire che le informazioni e i dati contenuti nel certificato siano esatti;
- **condizioni di utilizzo:** il richiedente è stato informato dal LRA-Officer in merito ai diritti e agli obblighi descritti nel presente documento. Il LRA-Officer della SG-PKI ha risposto in modo chiaro alle domande del richiedente a tale proposito. Il richiedente ha letto il documento, ne ha preso atto e lo ha firmato;
- **stato:** la SG-PKI rende disponibili online 7 giorni su 7, 24 ore su 24 lo stato del certificato e le informazioni relative alla sua validità e revoca conformemente alle disposizioni della FiEle, dell'OFiEle e di altre disposizioni legali;
- **revoca:** se del caso, la SG-PKI può revocare immediatamente il certificato in presenza di uno dei motivi citati nel presente documento.

Alla medesima persona giuridica possono essere rilasciati più certificati. Le richieste possono essere presentate dalla stessa persona autorizzata.

La chiave privata da utilizzare con il servizio di firma è salvata su un HSM, per cui è possibile autorizzare più utenti tramite il loro certificato personale di classe B o MobileID personale oppure, in caso di applicazioni specifiche, memorizzare un certificato TLS comune

nell'applicazione. Il certificato TLS memorizzato, che permette di utilizzare il certificato di firma vero e proprio per una persona giuridica, e i relativi dati di accesso possono essere trasmessi dal richiedente ai collaboratori rispettando la procedura prevista. In questo caso il richiedente, agendo per conto della persona giuridica, è responsabile in prima persona. La trasmissione dei dati di accesso deve essere annotata per scritto, in modo tracciabile e completo. Le applicazioni specifiche che richiedono l'autenticazione tramite un certificato TLS possono essere collegate al servizio di firma soltanto dopo essere state sottoposte a verifica da parte di un servizio esterno.

In caso di utilizzo di MobileID, le condizioni d'usoⁱⁱ separate di MobileID sono parte integrante del presente documento.

Il richiedente risponde di qualsiasi danno causato a terzi dalla trasmissione dei dati di accesso alla chiave privata e di eventuali dispositivi ad essa associati.

Il richiedente garantisce di conoscere il contenuto, lo scopo e le conseguenze dell'utilizzo del certificato regolamentato di classe A e che eventuali altri utenti autorizzati ne siano altresì a conoscenza. Inoltre, si impegna a utilizzare il certificato di classe A e la relativa chiave privata nel rispetto delle prescrizioni legali vigenti come pure delle disposizioni del presente documento. Il richiedente è tenuto a informare in modo esaustivo e comprovabile i contenuti in merito alle disposizioni e al contenuto del presente documento.

La firma viene apposta mediante il certificato e un software di firma. Al momento dell'approvazione del presente documento, le applicazioni raccomandate a tal fine dalla SG-PKI sono DesktopSigner e il servizio di firma dell'UFIT. La firma è verificata dal destinatario con l'ausilio del «validatore» online^{iv}. Una firma elettronica è considerata valida soltanto se provvista della marca temporale elettronica qualificata. Per garantire una convalida a lungo termine (LTV) si raccomanda di apporre la firma conformemente allo standard LTV, ossia di applicare sempre anche una marca temporale. La marca temporale può essere richiesta alla SG-PKI (Time-Stamping-Authority, TSA).

In caso di domande o problemi nell'utilizzo dei certificati ci si può rivolgere al Service Desk locale o al Service Desk dell'UFIT (tel.: 058 465 88 88). In caso di ricorso o di domande riguardanti il presente documento si prega di contattare la SG-PKI all'indirizzo e-mail servicedesk@bit.admin.ch.

4.1 Disponibilità

La SG-PKI garantisce l'esercizio dei servizi di certificazione e di stato (Online Certificate Status Protocol, OCSP; Certificate Revocation List, CRL) con una disponibilità conforme agli accordi SLA interni.

I lavori di manutenzione vengono pianificati in modo da non compromettere la disponibilità dei servizi. Le interruzioni necessarie sono rese note in anticipo tramite gli adeguati canali di comunicazione.

La SG-PKI gestisce i componenti rilevanti ai fini della sicurezza in conformità alle norme ETSI EN 319 401 ed EN 319 411-1 e garantisce che i tempi di interruzione siano ridotti al minimo e i guasti siano trattati tempestivamente.

La disponibilità menzionata si riferisce alle fasce orarie principali dei «trust service» e non include le finestre di manutenzione programmata. Sono fatte salve le interruzioni dovute a motivi di sicurezza.

5 Comunicazione e revoca

Il titolare si impegna a non utilizzare più il certificato e la relativa chiave privata o a non autorizzarne più l'utilizzo e a ritirarlo senza indugio nonché a chiederne immediatamente la revoca (annullamento) al TSP (ad es. LRA-Officer della SG-PKI nell'organizzazione del titolare) se:

- sussiste il sospetto concreto che un certificato sia stato usato per attività dubbie (compromissione/utilizzo illecito del certificato di firma);

- le informazioni contenute nel certificato non sono aggiornate o esatte o non lo saranno più entro breve;

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

Il richiedente originario può chiedere in ogni momento la revoca del certificato presentandosi di persona, inviando un'e-mail con firma digitale o per telefono. Il TSP o la persona da esso incaricata (ad es. LRA-Officer) verificherà inequivocabilmente l'identità del titolare.

Le altre persone autorizzate a chiedere una revoca devono presentare una richiesta scritta utilizzando l'apposito modulo online.

Le persone autorizzate sono:

- il titolare stesso (per le persone giuridiche: una persona autorizzata mediante procura e appartenente alla persona giuridica);
- il richiedente originario;
- i superiori gerarchici del titolare o del richiedente;
- il responsabile della SG-PKI;
- un responsabile della sicurezza della SG-PKI;
- il LRA-Officer competente della SG-PKI;
- l'incaricato della sicurezza informatica dell'unità amministrativa (ISIU);
- in caso di certificati per persone fisiche: i collaboratori del servizio del personale competente per il titolare.

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 quali fonti di attività dubbie.

Per ragioni di tracciabilità il TSP archivia tutte le informazioni legate alla revoca conformemente alle prescrizioni di legge.

Subito dopo il blocco è possibile presentare al TSP la richiesta per l'ottenimento di un nuovo certificato. La procedura per il rilascio di un nuovo certificato si svolge secondo le stesse modalità di quella per il primo rilascio.

6 Cessazione dell'utilizzo del certificato

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

7 Responsabilità

Il titolare deve garantire che il suo certificato di classe A e la relativa chiave privata siano utilizzati nel rispetto delle prescrizioni legali vigenti e delle disposizioni indicate al paragrafo «Utilizzo del certificato» del presente documento. Una violazione di questa prescrizione comporta la revoca del certificato ed eventualmente altre misure di natura amministrativa e giuridica. Il titolare è responsabile di tutte firme da lui apposte nonché di eventuali danni e conseguenze derivanti da un utilizzo non consentito.

Se viola gli obblighi imposti dalla FiEle e dalle relative disposizioni d'esecuzione, la SG-PKI risponde del danno causato al titolare del certificato e ai terzi che si sono fidati di un certificato valido ai sensi dell'articolo 17 FiEle.

La responsabilità della SG-PKI è limitata conformemente al diritto applicabile:

- in caso di violazione del contratto, risponde del danno comprovato, salvo non provi che non le è imputabile alcuna colpa;

- in caso di negligenza grave, risponde fino a 100 000 franchi per danno e anno civile;
- in caso di negligenza lieve, risponde del controvalore delle prestazioni fornite durante l'anno contrattuale in corso, fino a un massimo di 50 000 franchi per danno e anno civile.

La SG-PKI declina qualsiasi altra responsabilità. In particolare non è responsabile dei danni derivanti da un utilizzo del certificato da parte del titolare per scopi diversi da quelli previsti nelle prescrizioni legali vigenti e nelle disposizioni indicate al paragrafo «Utilizzo del certificato» del presente documento.

La SG-PKI declina espressamente la responsabilità per danni indiretti, perdita di guadagno e perdita di dati.

Inoltre, la SG-PKI non risponde in caso di danni e conseguenze della mora derivanti da cause di forza maggiore, eventi naturali (ad es. fulmini o cataclismi), black out, eventi bellici, scioperi, restrizioni impreviste dettate dalle autorità, elusione di set di blocco, PC-dialer, attacchi di hacker e virus (compresi trojan e simili) ad attrezzature informatiche e simili. Se la SG-PKI non può ottemperare ai propri obblighi contrattuali a causa di un evento di questo tipo, l'adempimento del contratto o il termine per l'adempimento vengono posticipati in funzione dell'evento occorso. La SG-PKI non risponde di eventuali danni arrecati al cliente a causa della proroga dell'adempimento del contratto.

8 Basi giuridiche, validità dei documenti ed elementi del contratto

Le basi giuridiche e le altre disposizioni indicate di seguito sono parte integrante delle presenti condizioni contrattuali e di utilizzo. Sono elencate nell'ordine in cui vengono applicate:

- 1) legge sulla firma elettronica (FiEle; RS 943.03);
- 2) ordinanza sulla firma elettronica (OFiEle; RS 943.032);
- 3) ordinanza dell'UFCOM sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (RS 943.032.1);
- 4) legge federale sul numero d'identificazione delle imprese (RS 431.03);
- 5) SG-PKI – Root CA IV – CP_CPS EN^v
- 6) il presente documento «Condizioni contrattuali e di utilizzo per i certificati di classe A – Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)».

Quando si utilizza MobileID: le condizioni d'uso di MobileID ⁱⁱ

Le disposizioni di legge vigenti, le policy e le direttive per certificati regolamentati e qualificati di classe A sono pubblicate o indicate sul sito Internet della SG-PKIⁱ.

8.1 Foro competente e diritto applicabile

A tutti i servizi offerti dalla SG-PKI è applicabile unicamente il diritto svizzero.

Il foro competente per tutte le controversie concernenti le presenti condizioni contrattuali o la loro applicazione è quello di Berna.

8.2 Reclami e controversie

I reclami relativi ai servizi di fiducia forniti dalla SG-PKI possono essere presentati da qualsiasi persona o organizzazione interessata.

La procedura comprende le fasi esposte qui di seguito.

- a) **Presentazione del reclamo**
I reclami devono essere inviati per scritto o e-mail ai recapiti del TSP elencati al numero 14.
- b) **Conferma della ricezione**
La SG-PKI conferma la ricezione entro cinque giorni lavorativi.

- c) **Verifica**
La SG-PKI esamina il caso in conformità con le direttive interne in materia di sicurezza, protezione dei dati e compliance.
- d) **Decisione / misure**
La decisione è notificata per scritto e motivata.
- e) **Escalation**
Le controversie che non possono essere risolte tramite la procedura di reclamo soggiacciono alle disposizioni esposte al numero 8.1 «Foro competente e diritto applicabile».

La SG-PKI si adopera per risolvere le controversie entro un termine congruo.

8.3 Verifica della conformità con CP/CPS

La SG-PKI si assicura che tutti i certificati emessi e i relativi processi soddisfino le direttive per la certificazione (Certificate Policy, CP) e le disposizioni di esecuzione delle stesse (Certification Practice Statement, CPS) applicabili.

La conformità è garantita nel seguente modo:

- controlli interni regolari (almeno 1 volta all'anno) sulla base delle disposizioni definite nelle CP e nelle CPS;
- audit esterni, svolti da un organismo indipendente di valutazione della conformità accreditato dal SAS secondo la norma ETSI EN 319 403;
- monitoraggio dei processi rilevanti per la sicurezza comprese la registrazione, l'identificazione, la gestione delle chiavi e l'emissione del certificato.

Le CP e le CPS sono pubblicate sul sito Internet della SG-PKI¹. Eventuali modifiche vengono documentate e pubblicate in base alla versione.

In caso di divergenze tra le presenti condizioni di utilizzo e le CP/CPS, prevalgono queste ultime.

9 Contenuto e validità dei certificati regolamentati e qualificati di classe A

I certificati della SG-PKI contengono informazioni riguardanti:

- il certificato radice dell'autorità di certificazione e l'autorità di certificazione responsabile del rilascio;
- le informazioni sulle policy vigenti;
- la data di rilascio e di scadenza del certificato;
- il numero di serie del certificato;
- l'elenco delle revoke dei certificati e il protocollo di stato del certificato online;
- le informazioni sul titolare del certificato, ovvero:
 - cognome e nome così come indicati nel documento di viaggio o d'identità oppure numero IDI e nome ufficiale del titolare in caso di persone giuridiche;
 - «common name» del titolare (cognome(i), nome(i) e suffisso);
 - l'indirizzo e-mail;
- la chiave pubblica.

Il certificato è valido al massimo per tre anni. Il titolare non può rinnovarlo autonomamente. Alla scadenza dei tre anni, il TSP deve rilasciarne uno nuovo, procedendo a una nuova verifica dell'identità del titolare. La procedura di rinnovo si svolge secondo le stesse modalità del primo rilascio. A tal fine il titolare deve presentarsi personalmente con la documentazione necessaria affinché sia possibile verificare la sua identità.

10 Informazioni per «relying parties»

Le «relying parties» (RP) che fanno affidamento su un certificato della SG-PKI sono tenute a verificarne la validità e l'integrità prima di utilizzarlo.

A tal fine, la SG-PKI mette a disposizione le seguenti informazioni e servizi:

- **periodo di validità:** i certificati della classe A hanno una validità massima di tre anni. Le date di rilascio e di scadenza sono contenute direttamente nel certificato;
- **informazioni sullo stato:** l'attuale stato di un certificato (valido, bloccato, scaduto) può essere consultato in ogni momento tramite l'OCSP o il CRL. I servizi di stato sono disponibili 24 ore su 24 e 7 giorni su 7;
- **verifica della firma:** una firma elettronica qualificata è valida soltanto se è provvista di una marca temporale qualificata. La verifica della firma può essere effettuata tramite il validatore^{iv} della Confederazione.

Le RP devono assicurarsi di utilizzare sempre dati aggiornati quando verificano un certificato e di rispettare le disposizioni delle leggi e delle norme applicabili (in particolare FiEle, OFiEle ed ETSI EN 319 401/411-1).

11 Richiesta e ottenimento di certificati di classe A

Per ottenere i certificati di classe A della SG-PKI è necessario presentare i documenti e operare le iscrizioni elencati di seguito:

- **Certificati qualificati per persone fisiche**
Per ottenere i certificati qualificati di classe A della SG-PKI è necessario presentare i documenti e operare le iscrizioni elencati di seguito:
 - un documento di viaggio valido per l'entrata in Svizzera (carta d'identità o passaporto), rilasciato al futuro titolare;
 - il modulo di richiesta per certificati qualificati di classe A della SG-PKI compilato e firmato elettronicamente almeno con un certificato di classe B;
 - l'iscrizione nell'Admin-Directory dell'Amministrazione federale che riporti cognome(i), nome(i) così come indicati nel documento di viaggio e l'indirizzo e-mail;
 - il presente documento «Condizioni contrattuali e di utilizzo per i certificati di classe A – Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)» firmato.

Per verificare inequivocabilmente l'identità del futuro titolare vengono accertate la validità, la correttezza e l'autenticità del suo documento di viaggio e che la foto corrisponda alla persona che si è presentata. Infine, prima di rilasciare un certificato personale qualificato occorre anche verificare la plausibilità della richiesta, accertandosi che il futuro titolare lavori effettivamente nell'unità organizzativa indicata nell'Admin-Directory, che necessiti del certificato per la sua attività professionale quotidiana e che sia autorizzato a richiederlo.

- **Certificati regolamentati per persone giuridiche**
Per ottenere i certificati regolamentati di classe A della SG-PKI è necessario presentare i seguenti documenti e operare le iscrizioni che attestino quanto segue:
 - il futuro titolare è un'unità IDI ai sensi dell'articolo 3 capoverso 1 lettera c della legge federale del 18 giugno 2010 sul numero d'identificazione delle imprese (LIDI);
 - il richiedente è autorizzato a firmare per conto della rispettiva unità IDI. L'autorizzazione deve essere comprovata da un estratto autenticato del registro di commercio o da una procura provvista di firma giuridicamente valida;
 - il modulo di richiesta per certificati regolamentati di classe A della SG-PKI compilato e firmato dal richiedente. Quest'ultimo può firmare la richiesta elettronicamente tramite il suo certificato personale di firma qualificato di classe A;

- il presente documento «Condizioni contrattuali e di utilizzo per i certificati di classe A – Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)» firmato dal richiedente;
- un documento di viaggio valido per l'entrata in Svizzera (carta d'identità o passaporto), rilasciato al richiedente.

Per il rilascio del certificato è necessario che il richiedente si presenti di persona. Per identificare il richiedente, al momento del rilascio i LRA-Officer di classe A della SG-PKI verificano la validità, l'esattezza e l'autenticità del suo documento di viaggio. Inoltre, i LRA-Officer devono accertarsi che la foto riportata sul documento d'identità corrisponda alla persona che hanno di fronte. Infine, prima di rilasciare un certificato regolamentato di classe A per persone giuridiche occorre anche verificare la plausibilità della richiesta, accertandosi che il richiedente lavori effettivamente nell'unità organizzativa indicata, che sia autorizzato a richiederlo e che necessiti del certificato per la sua attività professionale quotidiana.

Se sono necessarie ulteriori informazioni, il richiedente deve inoltrarle alla SG-PKI entro 10 giorni, trascorsi i quali la richiesta decade automaticamente.

12 Conservazione dei registri («event log»)

Nell'esercizio dei «trust service», la SG-PKI tiene registri degli eventi completi («event log») relativi alle procedure rilevanti ai fini della sicurezza. Questi comprendono in particolare:

- eventi di registrazione e di identificazione;
- rilasci e revoche di certificati;
- eventi di sistema dei componenti rilevanti per la sicurezza;
- accessi a hardware crittografici.

Conformemente ai requisiti di ETSI EN 319 401, numero 6.2, gli «event log» vengono conservati in modo da non poter essere manipolati e per una durata minima di 11 anni dallo scadere della validità del certificato interessato.

La conservazione dei registri serve a garantire la tracciabilità di eventi rilevanti per la sicurezza, a supportare i processi di audit e adempiere gli obblighi legali della prova.

L'accesso agli «event log» è limitato alle persone autorizzate ed è effettuato unicamente per scopi di sicurezza, audit, compliance e prova legale.

13 Dichiarazione di riconoscimento e di consenso

Il richiedente prende atto del fatto che il TSP revoca immediatamente il certificato in caso di sospetto fondato di utilizzo illecito, di inosservanza delle disposizioni del presente documento o di un'altra violazione delle prescrizioni legali vigenti.

Con la sua firma elettronica nella domanda, il richiedente conferma di aver letto e compreso il presente documento «Condizioni contrattuali e di utilizzo per i certificati di classe A – Certificati regolamentati e qualificati secondo la FiEle (per persone fisiche e giuridiche)» e di accettare le disposizioni ivi contenute.

14 Contatti del TSP

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

Indirizzo: Eichenweg 1 + 3, 3003 Berna

Telefono: +41 58 465 88 88

e-mail: servicedesk@bit.admin.ch

Sito Internet: www.pki.admin.ch

ⁱ Sito Internet Swiss Government PKI: <https://www.pki.admin.ch>

ⁱⁱ Condizioni d'uso MobileID: <https://www.mobileid.ch/it/documenti>

ⁱⁱⁱ Registro IDI: <https://www.uid.admin.ch/Pages/search.aspx?lang=it>

^{iv} Validatore della Confederazione: [Signature Validator – Validare il documento](#)

^v CP/CPS Swiss Government PKI: http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf