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[1].

Common name (CN):

Data di rilascio: **Firma:** _____

[1] 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).