Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze

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

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»[1]) 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

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

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.

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: _____