P.b.b. Ufficio postale del Poligrafico 1030 Vienna WoGZ 213U

GAZZETTA UFFICIALE

DELLA REPUBBLICA FEDERALE D'AUSTRIA

Anno 2000 **Pubblicata il 2 febbraio 2000** **Parte II**

Regolamento n. 30: Regolamento sulla firma elettronica – SigV

Regolamento n. 30 sulla firma elettronica – SigV, emanato dal Cancelliere federale

Visto il § 25 della Legge sulla firma digitale n. 190/1999 pubblicata nella Gazzetta ufficiale I, d'intesa con il Ministro federale della giustizia si dispone:

Indice

Commissioni per le attività di vigilanza

§ 1. (1) Per le attività individuali dell'autorità di vigilanza e di Telekom-Control GmbH, elencate qui in basso, i certificatori devono corrispondere le seguenti commissioni:

1. controllo e registrazione di un certificatore in occasione della denuncia di inizio attività (§ 6 comma 2 SigG)
   a) se il certificatore non emette certificati qualificati e non propone procedure per la generazione di firme elettroniche sicure 100 euro;
   b) se il certificatore emette certificati qualificati o propone procedure per la generazione di firme elettroniche sicure 6 000 euro;
2. controllo di un certificatore in occasione della denuncia di un ulteriore progetto di sicurezza e certificazione
   a) se il certificatore non emette certificati qualificati e non propone procedure per la generazione di firme elettroniche sicure: 50 euro;

b) se il certificatore emette certificati qualificati o propone procedure per la generazione di firme elettroniche sicure:	
aa) all'atto della denuncia di un ulteriore progetto di sicurezza e certificazione con variazioni rilevanti per la sicurezza	4 000 euro;
bb) all'atto delle denuncia di un ulteriore progetto di sicurezza e certificazione senza variazioni rilevanti per la sicurezza	1 000 euro;
3. controllo di un certificatore in occasione della sua domanda di accreditamento (§ 17 SigG)	6 000 euro;
4. controllo di un certificatore che emette certificati qualificati in caso di denuncia di variazioni fondamentali e rilevanti per la sicurezza di un progetto di sicurezza e certificazione preesistente (§ 6 comma 5 SigG)	4 000 euro;
5. a) controllo periodico di certificatore (§ 13 comma 1 SigG)	4 000 euro;
b) controllo supplementare di un certificatore se viene accertata una violazione non irrilevante delle disposizioni della Legge sulla firma elettronica o dei relativi regolamenti	6 000 euro;
c) controllo di un certificatore in caso di variazioni rilevanti per la sicurezza di un progetto di sicurezza e certificazione, nella misura in cui non siano state denunciate all'autorità di vigilanza	6 000 euro;
6. condizioni imposte in caso di vizi rilevanti per la sicurezza (§ 14 comma 6 SigG)	1 000 euro;
7. divieto dell'esercizio dell'attività di un certificatore (§ 14 commi 2-4 SigG)	1 000 euro;
8. controllo della sospensione dell'attività di un certificatore (§ 12 SigG)	100 euro;
9. prosecuzione del servizio di revoca di un certificatore da parte dell'autorità di vigilanza (§ 12 e § 14 comma 5 SigG)	1 euro l'anno per ogni certificato registrato nel servizio di revoca
10. tenuta degli elenchi presso l'autorità di vigilanza (§ 13 comma 3 e § 17 comma 1 SigG)	500 euro l'anno per ogni certificatore;
11. valutazione dell'equivalenza di verbali di controllo di un organismo riconosciuto di un Paese terzo (§ 24 comma 3 SigG)	6 000 euro.

(2) Per la copertura delle spese correnti fisse dell'autorità di vigilanza e di Telekom-Control GmbH, i certificatori che emettono certificati qualificati devono corrispondere una commissione di 2 euro l'anno per ogni certificato qualificato emesso e valido.

(3) Se nell'ambito dell'attività di vigilanza prevista dalla Legge sulla firma elettronica o dai relativi regolamenti, l'autorità di vigilanza o Telekom-Control GmbH si servono di un organismo di convalidazione o di altre persone o organizzazioni non ufficiali, le loro commissioni vengono stabilite ai sensi del § 53a della Legge generale sul procedimento amministrativo (AVG) e imposte al certificatore in questione come pagamento in contanti ai sensi del § 76 AVG.

(4) Le commissioni vengono imposte dall'autorità di vigilanza mediante avviso. Le commissioni di cui al comma 2 vengono riscosse pro quota a posteriori per ogni trimestre. A tale scopo i certificatori che emettono certificati qualificati devono notificare all'autorità di vigilanza entro il 15 di ogni mese il numero dei certificati qualificati emessi che erano validi il primo giorno del mese.

Dotazione finanziaria dei certificatori

§ 2. (1) I mezzi finanziari regolarmente disponibili per l'esercizio dell'attività di certificatore vanno notificati all'autorità di vigilanza contestualmente alla denuncia di inizio attività ai sensi del § 6 comma 2 SigG. La dotazione finanziaria minima dei certificatori che emettono certificati qualificati deve essere di 300 000 euro. Questo capitale minimo deve essere disponibile in forma di capitale proprio ai sensi del § 224 comma 3A e B del Codice commerciale. Per capitale nominale ai sensi del § 224 comma 3A del Codice commerciale si intende il capitale versato ai sensi del § 23 comma 3 della Legge federale sulla valutazione (BWG).

(2) I certificatori che emettono certificati qualificati devono altresì comprovare all'autorità di vigilanza, contestualmente alla denuncia di inizio attività ai sensi del § 6 comma 2 SigG, la stipula di

un'assicurazione di responsabilità civile con un massimale minimo di 1 000 000 euro per ogni caso assicurato.

(3) Lo stato federale, i Länder, le associazioni comunali e i comuni con più di 50 000 abitanti sono liberati dalle obbligazioni di cui ai commi 1 e 2.

Generazione di dati per la generazione di firme elettroniche sicure

§ 3. (1) I dati per la generazione della firma dell'autorità di vigilanza devono essere conformi all'**Appendice 1** punto 1 (sistema principale). Il sistema di generazione deve essere tenuto isolato, destinato esclusivamente a questo scopo e adeguatamente protetto da interventi esterni e turbative. Oltre ai propri dati per la generazione della firma, l'autorità di vigilanza deve generare un secondo sistema di dati di generazione della firma (seconda chiave) ed eseguire tutte le proprie firme elettroniche apposte sugli elenchi da essa tenuti anche con questo secondo sistema come backup. I dati per il controllo della firma (chiave pubblica) del secondo sistema vanno firmati con i dati per la generazione della firma dell'autorità di vigilanza. Il secondo sistema va tenuto sotto chiave. I dati per il controllo della firma del secondo sistema vanno utilizzati esclusivamente in caso di guasto al sistema principale, onde garantire il regolare funzionamento dei servizi di firma e certificazione dell'autorità di vigilanza anche in casi di questo genere. Se l'autorità di vigilanza utilizza aggiuntivamente anche dati per la generazione della firma diversi da quelli indicati al punto 1 dell'Appendice 1, i certificati che contengono i corrispettivi dati per il controllo della firma vanno firmati con il sistema principale ed essere pubblicamente consultabili in qualsiasi momento per via elettronica. L'autorità di vigilanza deve garantire che i dati impiegati per la generazione della firma e quelli per il controllo della firma del rispettivo certificato siano utilizzabili in modo complementare.

(2) I dati per la generazione della firma dei certificatori devono essere generati nella loro unità di generazione e non devono abbandonare tale unità. I dati per il controllo della firma generati devono essere notificati all'autorità di vigilanza nel progetto di sicurezza e certificazione del certificatore. Per il resto sono validi i requisiti delle firme elettroniche sicure degli altri firmatari.

(3) I dati per la generazione di firme elettroniche sicure dei firmatari devono avere la lunghezza minima stabilita al punto 2 dell'Appendice 1. Nel progetto di sicurezza del certificatore va specificata la lunghezza effettiva della chiave delle procedure di firma proposte, con indicazione del valore limite superiore e inferiore. Gli algoritmi impiegati vanno resi noti. I dati per la generazione di firme elettroniche sicure devono comparire esclusivamente presso il firmatario con un margine di probabilità ai limiti della certezza e permettere, in base allo stato della tecnica, di risalire chiaramente al firmatario stesso. La generazione ripetuta di dati per la generazione di firme elettroniche sicure non deve comportare una riduzione della qualità delle chiavi, nel rispetto del livello di sicurezza facente fede per la rispettiva procedura di firma.

(4) Applicazioni ripetute di dati per la generazione di firme elettroniche sicure non devono comportare una riduzione della qualità delle chiavi. Eventuali applicazioni in grado di ridurre la qualità dei dati per la generazione delle firme (ad esempio applicazioni RSA su dati scelti casualmente) vanno efficacemente escluse. I dati per la generazione della firma vanno impiegati esclusivamente per la loro specifica destinazione d'uso.

(5) La generazione dei dati per la generazione di firme elettroniche sicure deve basarsi su una casualità effettiva, basata a sua volta su una casualità tecnica o su una casualità riferita al firmatario. I dati per la generazione della firma devono essere influenzati da elementi casuali effettivi nel numero di posizioni di bit stabilite al punto 3 dell'Appendice 1 (casualità qualificata). L'idoneità degli elementi casuali deve essere adeguatamente controllata. Come base di partenza non si devono utilizzare numeri pseudocasuali. Se il sistema di generazione viene impiegato per i dati di generazione della firma di differenti firmatari, la qualità statistica della casualità tecnica impiegata va controllata periodicamente, almeno a cadenza mensile. I verbali di controllo vanno documentati. Se il controllo dà esito negativo, i certificati che si basano sui dati in questione, emessi dalla data dell'ultimo controllo superato con esito positivo, vanno revocati.

(6) Se i dati per la generazione di firme elettroniche sicure vengono generati presso il certificatore, quest'ultimo deve adottare misure atte ad escludere la divulgazione di questi e di altri dati dai quali si possano ricostruire i dati per la generazione della firma, nonché atte ad escludere la memorizzazione di tali dati all'esterno dell'unità di generazione della firma del firmatario. Lo stesso dicasi per il trasferimento di questi dati all'unità di generazione del firmatario e per i dati di

identificazione del firmatario verso l'unità di generazione della firma (ad esempio i PIN). Se i dati per la firma vengono generati all'esterno dell'unità di generazione del firmatario, si devono utilizzare sistemi di generazione adeguatamente protetti da interventi esterni e turbative. L'accesso al sistema di generazione deve essere sorvegliato, ogni utilizzatore va identificato e ogni utilizzo va registrato.

(7) Se i dati per la generazione di firme elettroniche sicure vengono generati nell'unità di generazione del firmatario, il certificatore deve proporre o raccomandare esclusivamente unità tecnicamente idonee per la generazione e la memorizzazione di tali dati.

Memorizzazione di dati per la generazione di firme elettroniche sicure

§ 4. (1) I dati per la generazione di firme elettroniche sicure vanno memorizzati in modo tale da escludere la loro divulgazione e garantire che il loro impiego sia sotto il controllo esclusivo del firmatario. Non è ammessa la duplicazione di questi dati dopo la loro generazione.

(2) I dati per la generazione di firme elettroniche sicure possono essere ripartiti, per particolari motivi di sicurezza, su più unità di generazione della firma. In questo caso, tutte le unità in questione devono soddisfare i requisiti di sicurezza. Il firmatario deve essere informato circa le misure necessarie per l'avvio della funzione di firma (§ 10 comma 7).

Infrastrutture e procedure tecnologiche dell'autorità di vigilanza

§ 5. I sistemi impiegati dall'autorità di vigilanza, in particolare i prodotti e le procedure tecnologiche, devono soddisfare i requisiti validi per le firme elettroniche sicure. L'autorità di vigilanza deve impiegare esclusivamente gli algoritmi specificati nell'**Appendice 2**.

Infrastrutture e procedure tecnologiche dei certificatori che emettono certificati qualificati

§ 6. (1) I sistemi impiegati da un certificatore che emette certificati qualificati, specie i prodotti e le procedure tecnologiche, vanno documentati nella loro versione aggiornata e in maniera verificabile. L'esistenza di elementi dei sistemi non documentati e le differenze rispetto alla documentazione, da ritenersi rilevanti ai fini della sicurezza, vanno viste come compromissione delle misure di sicurezza. Questo vale anche nel caso in cui questi elementi dei sistemi non siano necessari per l'erogazione dei servizi di firma e certificazione. Se gli elementi dei sistemi che il certificatore utilizza per l'erogazione dei servizi di firma e certificazione vengono impiegati anche per altre attività, l'efficacia degli elementi per l'erogazione dei predetti servizi deve rimanere impregiudicata.

(2) Per la generazione di firme elettroniche sicure vanno impiegati i metodi hash riportati al punto 2 dell'Appendice 2. Gli algoritmi per la generazione del valore hash vanno considerati sicuri fino al momento specificato al punto 2 dell'Appendice 2. A completamento del valore hash si possono impiegare anche numeri pseudocasuali. Per la cifratura del valore hash vanno impiegati gli algoritmi riportati al punto 3 dell'Appendice 2. Gli algoritmi per la generazione della firma vanno considerati sicuri fino al momento specificato al punto 3 dell'Appendice 2. Se si impiegano algoritmi di firma che necessitano di numeri casuali (ad esempio DSA), è ammesso l'utilizzo anche numeri pseudocasuali.

(3) Un certificatore che emette certificati qualificati deve essere in grado di controllare le firme elettroniche in modo sicuro. Le procedure e gli algoritmi per il controllo delle firme formano un'unità logica con le procedure e gli algoritmi per la generazione delle firme e vanno documentati congiuntamente.

Infrastrutture e procedure tecnologiche degli utilizzatori per la generazione di firme elettroniche sicure

§ 7. (1) Per la generazione di firme elettroniche sicure, i firmatari devono impiegare esclusivamente i metodi hash e le procedure di cifratura del valore hash riportate ai punti 2 e 3 dell'Appendice 2.

(2) Le infrastrutture e procedure tecnologiche impiegate dai firmatari per la generazione di firme elettroniche sicure devono permettere la visualizzazione completa dei dati da firmare. Per i dati da firmare vanno impiegati esclusivamente i formati raccomandati dal certificatore. La specifica di questi formati deve essere di pubblico dominio. Non è ammessa la codificazione di modificazioni dinamiche o di dati non visibili nei formati che offrono anche questa possibilità. Il certificatore deve istruire gli utilizzatori o proporre loro dei metodi atti ad escludere la codificazione di modificazioni dinamiche o di dati non visibili.

(3) La funzione di firma nell'unità di generazione della firma del firmatario deve poter essere avviata unicamente dopo aver digitato i codici di autorizzazione (ad esempio PIN o impronta digitale). Al firmatario va comunicato il numero di firme attivato con un'autorizzazione immessa nella sua unità di generazione. La possibilità di venire abusivamente a conoscenza dei codici di autorizzazione deve essere praticamente esclusa in virtù della loro configurazione e mediante efficaci meccanismi di disabilitazione. Il medesimo codice di autorizzazione non deve poter essere utilizzato per differenti applicazioni (ad esempio funzione di firma e funzione Bancomat). È ammesso l'impiego di unità di generazione della firma che permettono più applicazioni, ad esempio carte o terminali multiapplicativi, se nel progetto di sicurezza sono descritte le misure e i metodi che impediscono l'attivazione di differenti applicazioni con i medesimi codici di autorizzazione. I codici di autorizzazione digitati non devono essere memorizzati dagli elementi dei sistemi impiegati. In caso di immissione ripetuta di codici di autorizzazione, si deve escludere la possibilità di ricorrere a procedure di immissione abbreviate. I codici di autorizzazione possono essere ripartiti su più elementi del sistema per aumentarne la sicurezza. Il firmatario va informato circa la procedura da seguire per l'attivazione della funzione di firma (§ 10 comma 7).

(4) I formati di firma particolarmente indicati sono quelli riportati al punto 4 dell'Appendice 2.

(5) Il destinatario di una dichiarazione firmata elettronicamente che intende effettuare un controllo sicuro della firma deve utilizzare unità di controllo definite come idonee nel progetto di sicurezza del certificatore che ha emesso il certificato. Queste unità di controllo della firma devono soddisfare i requisiti specificati al § 18 comma 4 SigG.

Protezione delle infrastrutture tecnologiche per la generazione di firme elettroniche sicure presso il certificatore

§ 8. Il certificatore deve adottare opportune misure atte a proteggere dalla compromissione e da interventi non autorizzati i dati per la generazione delle firme e le infrastrutture tecnologiche impiegate per l'emissione dei certificati e per la consultabilità dei servizi elenchi e di revoca. Gli interventi non autorizzati devono essere riconoscibili.

Controllo delle infrastrutture e procedure tecnologiche per certificati qualificati e firme elettroniche sicure

§ 9. (1) Per il controllo delle infrastrutture e procedure tecnologiche per certificati qualificati e firme elettroniche sicure si possono applicare profili di sicurezza (Protection Profiles) specificati nei Criteri comuni per il controllo e la valutazione della sicurezza nella tecnologia dell'informazione (Common Criteria for Information Technology Security Evaluation, ISO 15408), che siano idonei e riconosciuti da un organismo di convalidazione.

(2) Il controllo delle infrastrutture e procedure tecnologiche ai sensi del § 7 comma 2, § 10 e § 18 SigG, può essere effettuato anche secondo i Criteri di valutazione della sicurezza di sistemi della tecnologia dell'informazione (ITSEC), e, nella misura in cui applicabili, anche secondo i Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) oppure secondo il British Standard (BS) 7799. In caso di applicazione degli ITSEC, per la generazione e la memorizzazione di dati per la generazione della firma, per la generazione di firme elettroniche sicure ed eventualmente per il controllo sicuro delle firme occorre rispettare il livello di valutazione E 3 con giudizio minimo dei meccanismi di sicurezza "alto"; per le altre infrastrutture e procedure tecnologiche va rispettato il livello di valutazione E 2 con giudizio minimo dei meccanismi di sicurezza "alto".

(3) Nel certificato che attesta il rispetto dei requisiti di sicurezza delle infrastrutture e procedure tecnologiche va indicato per quali applicazioni, a quali condizioni e fino a quale data esso è valido. Un esemplare del verbale di controllo e del certificato va trasmesso all'autorità di vigilanza.

Erogazione di servizi di firma e certificazione per certificati qualificati e firme elettroniche sicure

§ 10. (1) Se le attrezzature di un certificatore che emette certificati qualificati vengono gestite separatamente sotto un profilo organizzativo o tecnico, occorre garantire, mediante l'adozione di opportune misure di sicurezza, che il trasferimento dei dati tra le singole attrezzature parziali non comporti una compromissione dei servizi di firma e certificazione.

(2) Le attrezzature tecniche di un certificatore vanno strutturate in modo tale che le funzioni ed applicazioni occorrenti per i servizi di firma e certificazione da erogare siano separate da altre funzioni ed applicazioni. Si deve escludere che altre funzioni ed applicazioni influiscano sui servizi di firma e certificazione. Questo va garantito sia per l'attività ordinaria, sia per situazioni di esercizio particolari ed anche al fuori dell'esercizio. Situazioni di esercizio particolari (ad esempio lavori di manutenzione) vanno documentate.

(3) Un certificatore che emette certificati qualificati deve adottare misure atte a proteggere da interventi non autorizzati le attrezzature che impiega per l'erogazione di servizi di firma e certificazione.

(4) Un certificatore che emette certificati qualificati non deve occupare per i servizi di firma e certificazione persone già condannate ad una pena detentiva superiore ad un anno per atti dolosi o ad una pena detentiva superiore a tre mesi per reati contro il patrimonio o per contraffazione di atti e prove. Non vengono considerate le condanne estinte ai sensi delle disposizioni della Legge sull'estinzione della pena del 1972 o soggette ad informazione limitata. Il certificatore deve controllare l'affidabilità del personale ad intervalli di almeno due anni.

(5) Il personale tecnico di un certificatore che emette certificati qualificati deve possedere adeguate conoscente tecniche nei seguenti settori:

1. preparazione informatica generale,
2. tecnologia di sicurezza, crittografia, firma elettronica e Public Key Infrastructure,
3. norme tecniche, in particolare norme sulla valutazione e
4. hardware e software.

Su richiesta dell'autorità di vigilanza, il certificatore deve illustrare il percorso di formazione presso strutture riconosciute o le esperienze professionali specifiche sulle quali si fonda il know how del personale. La formazione del personale tecnico nei vari settori deve essere durata almeno un anno. L'adeguato know how può essere stato acquisito ad esempio conseguendo il diploma di un Istituto tecnico superiore o di un politecnico oppure un diploma di laurea nelle discipline di merito. Questa preparazione può essere sostituita da un'esperienza professionale specifica di almeno tre anni.

(6) I dati per la generazione della firma generati presso il certificatore vanno consegnati esclusivamente al firmatario. Va esclusa la possibilità di utilizzo dei dati per la generazione della firma prima della loro consegna al firmatario. In ogni caso il certificatore deve accertarsi che i dati per la generazione della firma del firmatario e i dati per il controllo della firma del rispettivo certificato siano utilizzabili in modo complementare.

(7) Prima che i dati per la generazione della firma vengano utilizzati per la prima volta, il certificatore deve informare il firmatario per iscritto o mediante un supporto dati indelebile, in modo chiaro e generalmente comprensibile, in ordine a tutte le misure di sicurezza da adottare all'atto dell'utilizzo di quei dati (ad esempio sicurezza dei codici di autorizzazione, esclusione dell'uso improprio, ricorso ai servizi elenchi e servizi di revoca, possibilità di visualizzare i dati da firmare, impiego di formati idonei).

Domanda di emissione di un certificato qualificato

§ 11. (1) Il certificatore deve accertare l'identità del richiedente servendosi di un documento d'identità con fotografia valido. La domanda di emissione di un certificato qualificato deve recare la

firma autografa del richiedente. Del documento d'identità esibito si deve produrre una fotocopia che va documentata assieme alla domanda. Se tale domanda reca la firma elettronica sicura del richiedente, si può prescindere da una ripetizione dell'identificazione.

(2) La domanda di emissione di un certificato deve contenere in particolare:

1. nome, data e luogo di nascita, indirizzo del richiedente, data di emissione e numero del documento d'identità esibito e autorità emittente;
2. eventuali dati su possibili limitazioni dell'ambito d'impiego o del valore delle transazioni da inserire nel certificato;
3. eventuali dati sul potere di rappresentanza di terzi, altri requisiti di rilevanza giuridica del richiedente, ad esempio l'abilitazione all'esercizio di una professione o altre abilitazioni, oppure altri dati da inserire nel certificato qualificato.

(3) Se in un certificato qualificato vanno inseriti dati sul potere di rappresentanza di un terzo, tale potere va opportunamente documentato oppure va prodotta un'autorizzazione recante la firma elettronica sicura del terzo in questione, il quale va informato per iscritto o mediante un supporto dati indelebile, circa il contenuto del certificato qualificato e la possibilità di revoca ai sensi del § 9 comma 1 n. 1 SigG. Anche l'abilitazione all'esercizio di una professione o altra abilitazione va opportunamente documentata prima di essere inserita nel certificato. Se la qualifica professionale del firmatario rientra nella sfera di competenza di un'autorità di vigilanza di diritto pubblico, l'organismo che svolge l'attività di vigilanza va informato per iscritto o mediante un supporto dati indelebile, circa il contenuto del certificato qualificato.

Certificati qualificati

§ 12. (1) Se un certificatore emette, oltre a certificati qualificati, anche altri certificati, per la firma dei certificati qualificati deve utilizzare dati per la generazione della firma separati.

(2) Formati idonei per i certificati qualificati sono in particolare quelli indicati al punto 5 dell'Appendice 2. Lo stesso dicasi per le codificazioni nei certificati qualificati.

(3) Il periodo di validità di un certificato qualificato deve essere al massimo di tre anni e non superare il periodo di idoneità delle infrastrutture e procedure tecnologiche impiegate, nonché dei relativi parametri specificati nelle Appendici 1 e 2.

(4) Prima dello scadere di un certificato qualificato è ammesso ricertificare i medesimi contenuti e i medesimi dati per il controllo della firma, fatta eccezione per il periodo di validità, ed emettere così un nuovo certificato. In tutti gli altri casi i certificati con i medesimi dati per il controllo della firma e contenuti differenti producono una compromissione dei certificati in questione.

(5) Un certificatore ha la facoltà, previo consenso di un altro certificatore, di certificare il certificato di quest'ultimo o i certificati emessi da quest'ultimo. I certificati così emessi non devono presentare modificazioni; egli deve altresì curare i servizi elenchi e i servizi di revoca ed eventualmente attuare direttamente le revoche dell'altro certificatore.

Servizi elenchi e servizi di revoca per certificati qualificati

§ 13. (1) I formati particolarmente idonei per i servizi elenchi e servizi di revoca sono quelli indicati al punto 6 dell'Appendice 2. I servizi elenchi e i servizi di revoca possono essere predisposti anche in formati differenti. Il certificatore deve garantire che i formati dei servizi di revoca siano idonei ad un'eventuale prosecuzione del servizio da parte dell'autorità di vigilanza. I servizi elenchi e i servizi di revoca rilevati da un altro certificatore devono mantenere i medesimi formati.

(2) Il certificatore deve rendere note ai firmatari e a terzi per i quali vengono inseriti dati in un certificato qualificato, idonee possibilità di comunicazione con le quali poter disporre in qualsiasi momento la revoca immediata del certificato. A tale scopo va prevista una procedura di autenticazione. La revoca di un certificato qualificato deve comunque essere possibile anche in forma cartacea.

(3) I servizi elenchi e i servizi di revoca devono essere adeguatamente protetti da falsificazioni, manipolazioni e richiami abusivi. Occorre garantire che solamente le persone autorizzate possano

effettuare registrazioni e modificazioni degli elenchi. Va altresì esclusa la possibilità di annullare inavvertitamente un blocco o una revoca.

(4) I servizi di revoca vanno aggiornati, durante l'orario d'ufficio, entro tre ore dalla comunicazione della causa della revoca. L'orario d'ufficio deve andare quanto meno dalle ore 9 alle ore 17 nei giorni lavorativi e dalle ore 9 alle ore 12 nella giornata di sabato. Al di fuori degli orari d'ufficio il certificatore deve comunque garantire che la richiesta di revoca di un certificato qualificato possa essere ricevuta automaticamente in qualsiasi momento, provocandone il blocco.

(5) La disponibilità temporale dei servizi elenchi deve essere indicata nel progetto di sicurezza. I servizi elenchi devono essere disponibili quanto meno negli orari d'ufficio indicati al comma 4. I servizi di revoca devono essere disponibili costantemente. Un'interruzione continuata di oltre 30 minuti durante il periodo di disponibilità dei servizi elenchi o dei servizi di revoca va documentata come caso di non operatività. Per situazioni di manutenzione e non operatività del servizio di revoca va predisposto un sistema sostitutivo. Se un guasto interessasse anche il sistema sostitutivo, occorrerà darne comunicazione entro un giorno solare all'autorità di vigilanza, la quale dovrà ripristinare il servizio di revoca entro tre giorni solari. I servizi di revoca devono essere pubblicamente accessibili. La consultazione dei servizi di revoca deve essere gratuita e senza identificazione.

(6) Un certificatore deve gestire i servizi elenchi e i servizi di revoca quanto meno fino al momento della necessaria riapposizione della firma (§ 17). Scaduto questo termine, il certificatore deve consentire una verifica dei certificati qualificati, nel singolo caso, fino allo scadere del termine specificato al § 16 comma 2. Lo stesso dicasi per la prosecuzione dei servizi di revoca da parte dell'autorità di vigilanza in caso di sospensione o divieto dell'attività di un certificatore.

(7) Il periodo di efficacia di un blocco deve essere indicato nel progetto di sicurezza. Questo periodo non deve superare i tre giorni lavorativi. Durante questo periodo il blocco può essere annullato. Un blocco annullato non incide sulla validità del certificato. Il certificato va revocato se il blocco non viene annullato entro il predetto termine. Se un certificato viene revocato a seguito di un blocco, già il blocco di per sé è da considerarsi come revoca.

(8) Se i dati per la generazione della firma del firmatario diventano noti o se compaiono una seconda volta come dati per la generazione di una firma o in altra forma, si è in presenza di una loro compromissione che deve comportare la revoca del certificato del firmatario. La revoca va richiesta dal firmatario (§ 9 comma 1 n. 1 SigG) oppure attuata dal certificatore di propria iniziativa (§ 9 comma 1 n. 6 SigG) non appena viene a conoscenza della compromissione.

Servizi di time stamping sicuri

§ 14. (1) Per l'erogazione di servizi di time stamping sicuri vanno utilizzati esclusivamente certificati qualificati ed emessi unicamente a questo scopo. Tale destinazione d'uso va indicata nel certificato.

(2) La localizzazione temporale certificata (data e ora) deve uniformarsi all'ora dell'Europa centrale e tenere conto dell'ora legale; altri fusi orari vanno esplicitamente indicati. Eventuali differenze rispetto all'ora esatta devono essere al massimo di un minuto.

(3) La disponibilità temporale di servizi di time stamping sicuri deve essere indicata nel progetto di sicurezza del certificatore che propone servizi di questo genere.

Progetto di sicurezza e certificazione per certificati qualificati

§ 15. (1) Il progetto di sicurezza e certificazione deve contenere in particolare i seguenti dati:

1. nome del certificatore,
2. indirizzo del certificatore e stato dove ha sede,
3. tipo, ambito di applicazione ed erogazione dei servizi di firma e certificazione proposti,
4. procedura di domanda,
5. eventualmente tipo e modalità d'inserimento nel certificato di uno pseudonimo e di dati sul potere di rappresentanza o altri requisiti giuridicamente rilevanti del firmatario,
6. orari d'ufficio,
7. generazione dei dati per la generazione della firma del certificatore,
8. formato dei dati per la generazione della firma del certificatore,

9. dati per il controllo della firma, eventualmente il certificato del certificatore,
10. generazione dei dati per la generazione della firma dei firmatari,
11. formato dei dati per la generazione della firma dei firmatari,
12. procedure applicate per la generazione delle firme proposte (metodo hash e procedure per la cifratura del valore hash),
13. elenco dei prodotti per la firma impiegati, predisposti e raccomandati,
14. sicurezza dei codici di autorizzazione,
15. formati applicabili per i documenti da firmare ed eventualmente metodi per impedire modificazioni dinamiche,
16. formati e periodo di validità dei certificati,
17. norme tecniche, modalità di accesso e periodo di aggiornamento e disponibilità dei servizi elenchi e servizi di revoca, incluso il periodo del blocco,
18. eventualmente il periodo di disponibilità dei servizi di time stamping proposti,
19. metodo chiaro e generalmente comprensibile per il controllo sicuro della firma,
20. formato della documentazione delle misure di sicurezza, casi di non operatività e situazioni di esercizio particolari,
21. periodo e procedura di riapposizione della firma,
22. protezione delle infrastrutture tecnologiche contro l'accesso non autorizzato,
23. protezione delle attrezzature del certificatore contro l'accesso non autorizzato.

(2) Il progetto di sicurezza e certificazione va prodotto all'autorità di vigilanza in forma elettronica in formato RTF, PDF, ASCII o Postscript. Il progetto deve recare la firma elettronica sicura del certificatore. Il progetto di sicurezza e certificazione e un suo riepilogo devono essere consultabili in qualsiasi momento per via elettronica, in forma chiara e generalmente comprensibile, in formato RTF, PDF ASCII o Postscript.

Documentazione

§ 16. (1) La documentazione specificata al § 11 SigG, inclusa quella dei casi di non operatività, delle situazioni di esercizio particolari e dell'informazione al richiedente stabilita al § 20 SigG, deve essere comunque redatta in forma elettronica. Se i dati per la generazione della firma vengono generati all'esterno dell'unità di generazione della firma del firmatario, quanto sopra vale anche per il momento del trasferimento dei predetti dati all'unità di generazione. I dati contenuti nella documentazione di un certificatore che emette certificati qualificati devono recare la sua firma elettronica sicura e un time stamping sicuro (§ 14).

(2) La documentazione di cui al comma 1 va conservata almeno 33 anni dall'ultima registrazione e protetta in modo da essere leggibile e disponibile durante tutto questo arco di tempo.

Riapposizione della firma elettronica (post-firma)

§ 17. Il periodo trascorso il quale si dovrebbe apporre una nuova firma elettronica a causa della diminuzione incombente del grado di sicurezza, deve essere indicato nel progetto di sicurezza e certificazione del certificatore, il quale deve comunque prevedere una post-firma prima dello scadere dei periodi di sicurezza delle procedure impiegate per la generazione della firma, indicati nelle appendici. Quando si appone una nuova firma va applicato un time stamping.

Vigilanza e accreditamento

§ 18. (1) La denuncia di inizio attività di un certificatore ai sensi del § 6 comma 2 SigG deve avvenire in forma elettronica. Se particolari contenuti della denuncia non richiedono un altro formato, va utilizzato il formato RTF, PDF, ASCII o Postscript. La denuncia va firmata elettronicamente. L'autorità di vigilanza deve essere in grado di persuadersi dell'autenticità dei dati. A tal fine può anche disporre la comparizione del certificatore o di un organo con potere di rappresentanza. Se il certificatore emette certificati qualificati, l'autorità di vigilanza deve accertarsi della complementarietà tra i dati per la generazione della firma del certificatore e i dati per il controllo della firma del certificato corrispondente.

(2) Alla denuncia vanno allegati in particolare:
1. il progetto di sicurezza e certificazione,
2. la rappresentazione dei pericoli e rischi specifici, rilevanti per la sicurezza, presso il certificatore,

3. la dimostrazione della dotazione finanziaria e dell'assicurazione di responsabilità civile richiesta e
4. la dimostrazione del know how del personale tecnico.

(3) Le disposizioni di cui al comma 1 vanno applicate per analogia alla denuncia di altri progetti e alla denuncia di cambiamenti rilevanti per la sicurezza del progetto di sicurezza e certificazione esistente.

(4) L'autorità di vigilanza deve controllare periodicamente i certificatori ad intervalli di almeno due anni ed anche in caso di cambiamenti rilevanti per la sicurezza del progetto di sicurezza e certificazione. Inoltre l'autorità di vigilanza ha la facoltà di effettuare in qualsiasi momento controlli per campionamento dei certificatori. L'autorità di vigilanza deve procedere a tale controllo supplementare in caso di sospetto fondato dell'esistenza di vizi rilevanti per la sicurezza.

(5) L'autorità di vigilanza, i suoi organi e le persone e strutture che operano per suo conto sono soggetti al segreto d'ufficio ai sensi dell'art. 20 comma 3 della Legge costituzionale federale.

(6) Negli elenchi tenuti dall'autorità di vigilanza vanno registrate esclusivamente circostanze di veridicità provata. Per questi elenchi va impiegato uno dei formati specificati al punto 6 nell'Appendice 2. L'autorità di vigilanza deve avere una homepage pubblicamente consultabile, nella quale vanno indicati il suo indirizzo, i suoi dati per il controllo della firma, i formati degli elenchi da essa gestititi e le loro modalità di consultazione.

(7) In caso di accreditamento volontario ai sensi del § 17 SigG, la domanda di accreditamento sostituisce la denuncia di inizio attività del certificatore.

(8) La denominazione dei certificatori accreditati ai sensi del § 17 SigG deve contenere la formulazione "Certificatore accreditato". I certificatori accreditati sono autorizzati ad utilizzare l'emblema federale con la scritta "Certificatore accreditato".

Rimando alla notificazione

§ 19. Il presente Regolamento è stato notificato alla Commissione europea (notificazione n. 99/0448/A) in conformità alle disposizioni della Direttiva 98/34/CE sulla procedura d'informazione nel settore delle norme e prescrizioni tecniche nella versione della Direttiva 98/48/CE, emanata dal Parlamento europeo e dal Consiglio.

Klima

Appendice 1

Parametri delle infrastrutture e procedure tecnologiche per firme elettroniche sicure

1. Dati per la generazione della firma dell'autorità di vigilanza

I dati per la generazione della firma dell'autorità di vigilanza devono essere conformi alla metodo RSA (per la cifratura del valore hash) (sistema principale).

Se l'autorità di vigilanza si servisse anche di altri dati per la generazione della firma (§ 3 comma 1 penultima proposizione), questi ultimi devono essere dati per la generazione di firme elettroniche sicure.

2. Dati per la generazione di firme elettroniche sicure

La lunghezza della chiave dei dati per la generazione di firme elettroniche sicure deve essere di almeno
- 1023 bit per il metodo RSA,
- 1023 bit per il metodo DSA,
- 160 bit per varianti DSA basate su curve ellittiche.

I bit zero a sinistra non vanno calcolati nella lunghezza della chiave. La lunghezza della chiave è comunque determinante per la parte segreta dei dati per la generazione della firma.

3. Elementi casuali per dati per la generazione di firme elettroniche sicure

I dati per la generazione di firme elettroniche sicure devono essere influenzati da elementi casuali effettivi nel seguente numero di posizioni di bit:
- 1023 bit per i metodi RSA e DSA,
- 160 bit per varianti DSA basate su curve ellittiche.

In questi casi esiste una casualità qualificata.

Se per garantire l'unicità di dati per la generazione della firma vengono inseriti, all'atto della loro generazione, altri elementi della chiave, in forma prestabilita o casuale, ad esempio bit a sinistra o a destra, il numero di posizioni di bit che va influenzato da una casualità qualificata non deve subire riduzioni.

4. Periodo di sicurezza

Posto l'impiego dei predetti algoritmi, le lunghezze delle chiavi dei dati per la generazione della firma specificate ai punti 1-3, vanno considerate sicure per firme elettroniche sicure fino al 31 dicembre 2005.

Appendice 2

Procedure tecnologiche e formati

1. Procedure tecnologiche dell'autorità di vigilanza

Il metodo hash che l'autorità di vigilanza deve impiegare è il metodo SHA-1 e per la cifratura del valore hash il metodo RSA (sistema principale). Non è ammesso l'impiego del Chinese Remeinder Theorem (CRT).
Se l'autorità di vigilanza utilizza anche altri dati per la generazione della firma (§ 3 comma 1 penultima proposizione), occorre che i corrispettivi metodi di cifratura del valore hash siano metodi per firme elettroniche sicure.

2. Metodi hash per firme elettroniche sicure

I seguenti metodi hash sono riconosciuti come sicuri:
a) RIPEMD-160,
b) funzione SHA-1.
L'impiego di questi metodi hash per firme elettroniche è da considerarsi sicuro fino al 31 dicembre 2005.
A questi metodi hash sono equiparati altri metodi che forniscano quanto meno la medesima sicurezza e siano stati riconosciuti come tali e pubblicati da un organismo di convalidazione.

3. Metodi per la generazione di firme elettroniche sicure (cifratura del valore hash)

I seguenti metodi vengono riconosciuti sicuri per la generazione di firme elettroniche sicure:
a) RSA,
b) DSA,
c) varianti del metodo DSA basate su curve ellittiche:
   - ISO/IEC 14883-3, Allegato A 2.2 (Agnew-Mulin-Vanstone analogue"),
   - Standard IEEE P1363, capitolo 5.3.3 ("Nyberg-Rueppel version"),
   - Standard IEEE P1363 [5], capitolo 5.3.4 ("DSA version").

Per l'implementazione vanno applicati, nei limiti del possibile, metodi riconosciuti a livello internazionale.
L'impiego dei predetti algoritmi per firme elettroniche va considerato sicuro fino al 31 dicembre 2005.

A questi metodi per la generazione della firma sono equiparati altri metodi che forniscano quanto meno la medesima sicurezza e siano stati riconosciuti come tali e pubblicati da un organismo di convalidazione.

4. Formati per firme elettroniche sicure

I formati impiegati per firme elettroniche sicure dovrebbero essere conformi ad uno standard riconosciuto a livello internazionale o ad una raccomandazione internazionale (ad esempio PKCS#7 Cryptographic Message Syntax Standard).

5. Formati per certificati qualificati

La European Electronic Signatures Standardization Initiative (EESSI) sta elaborando formati e norme per la rappresentazione di certificati qualificati e per i loro contenuti. Per il momento si suggerisce l'applicazione di progetti di norma riconosciuti a livello internazionale (ad esempio X.509 v3 certificate oppure X.509 v2 CRL for use in the Internet). Le peculiarità del formato vanno descritte nel progetto di sicurezza e certificazione. Per tale descrizione va impiegata una Formale Notation (ad esempio CCITT risp. ITU-T Reccomendation X.208; Specification of Abstract Syntax Notation One - ASN.1 – 1988). Lo stesso dicasi per la codificazione dell'attributo "qualificato" in un certificato qualificato.

6. Formati per servizi elenchi e servizi di revoca per certificati qualificati

I servizi elenchi e servizi di revoca dovrebbero essere tenuti in un formato riconosciuto a livello internazionale.
Per l'accesso ai servizi elenchi e servizi di revoca si raccomandano in particolare le seguenti norme internazionali:
a) 1988 CCITT (ITU-T) X.500 / ISO IS9594,
b) RFC 2587 Internet X.509 Public Key Infrastructure LDAPv 2 Schema,
c) RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,
d) RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for Dynamic Directory Services.

Stampata da Print Media Austria AG (ex Österreichische Staatsdruckerei AG)