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

GAZZETTA UFFICIALE

DELLA REPUBBLICA FEDERALE D'AUSTRIA

Anno 1999 Pubblicata il 19 agosto 1999 Parte I

Legge federale n. 190: Legge sulla firma elettronica – SigG
(NR: GP ZZ RV 1999 AB 2065 p. 180.BR; AB 6065 p. 657)

Legge federale n. 190 sulla firma elettronica (SigG)

Il Consiglio nazionale ha decretato:

Sezione I.

Oggetto e definizioni

Oggetto e ambito di applicazione

§ 1. (1) La presente Legge federale disciplina il quadro giuridico per la generazione e l'utilizzo di firme elettroniche e per l'erogazione di servizi di firma e certificazione.

(2) La presente Legge federale si applica anche in sistemi chiusi purché i loro partecipanti lo abbiano pattuito, e nei rapporti elettronici pubblici con tribunali e altre autorità, salvo diversa disposizione di legge.

Definizioni

§ 2. Significato dei termini ricorrenti nella presente Legge federale:

1. firma elettronica: dati elettronici che vengono aggiunti ad altri dati elettronici o associati logicamente ad essi, i quali servono all'autenticazione, ovvero all'accertamento dell'identità del firmatario;
2. firmatario: una persona fisica alla quale sono stati assegnati dati per la generazione della firma e i relativi dati per il controllo della firma, e che genera una firma elettronica per proprio conto e per conto altrui, oppure un certificatore che utilizza certificati per l'erogazione di servizi di certificazione;
3. firma elettronica sicura: una firma elettronica che
   a) è associata esclusivamente al firmatario,
   b) permette l'identificazione del firmatario,
   c) viene generata con strumenti che il firmatario può tenere sotto il proprio esclusivo controllo,
   d) è collegata ai dati ai quali si riferisce in modo tale da poter accertare qualsiasi successiva modificazione dei dati stessi,
   e) si basa su un certificato qualificato e viene generata impiegando infrastrutture e procedure tecnologiche che soddisfano i requisiti di sicurezza stabiliti nella presente Legge federale e nei relativi regolamenti;
4. dati per la generazione della firma: dati unici, quali codici o chiavi private di firma, che il firmatario utilizza per la generazione di una firma elettronica;
5. unità di generazione della firma: un software configurato o un hardware che viene utilizzato per l'elaborazione dei dati di generazione della firma;
6. dati per il controllo della firma: dati quali codici o chiavi pubbliche di firma che vengono utilizzati per il controllo di una firma elettronica;
7. unità di controllo della firma: un software configurato o un hardware che viene utilizzato per l'elaborazione dei dati di controllo della firma;
8. certificato: un certificato elettronico con il quale si associano dati di controllo della firma ad una determinata persona e se ne conferma l'identità;

9. certificato qualificato: un certificato che contiene le informazioni di cui al § 5 e che viene emesso da un certificatore in possesso dei requisiti di cui al § 7;
10. certificatore: una persona fisica o giuridica oppure un'altra organizzazione avente personalità giuridica che emette certificati o eroga altri servizi di firma e certificazione;
11. servizi di firma e certificazione: la messa a disposizione di prodotti e procedure necessari per la firma, l'emissione, il rinnovo e la gestione di certificati, servizi elenchi, servizi di revoca, servizi di registrazione e servizi di time stamping, nonché servizi informatici e di consulenza correlati alle firme elettroniche;
12. servizio di time stamping: un'attestazione recante la firma elettronica di un certificatore che comprova l'esistenza di determinati dati elettronici in un determinato momento;
13. prodotto per la firma: un hardware o software o i loro componenti specifici che vengono utilizzati per la generazione ed il controllo di firme elettroniche oppure per l'erogazione di servizi di firma e certificazione da parte di un certificatore;
14. compromissione: il pregiudizio arrecato a misure di sicurezza o alla tecnologia di sicurezza, dal quale deriva il mancato raggiungimento del livello di sicurezza adottato dal certificatore.

Sezione II.

Firme elettroniche giuridicamente rilevanti

Effetti giuridici generali

§ 3. (1) Nei rapporti giuridici e commerciali si possono applicare procedure di firma con differenti livelli di sicurezza e differente categoria di certificato.

(2) L'efficacia giuridica di una firma elettronica e il suo utilizzo come mezzo probatorio non possono essere esclusi semplicemente in virtù del fatto che la firma esiste unicamente in forma elettronica, oppure perché non si basa su un certificato qualificato o su un certificato qualificato emesso da un certificatore accreditato oppure perché non è stata generata con le infrastrutture e procedure tecnologiche specificate al § 18.

Effetti giuridici speciali

§ 4. (1) Una firma elettronica sicura soddisfa il requisito di legge della firma autografa, specie il requisito della forma scritta ai sensi del § 886 del Codice civile generale austriaco (ABGB), salvo diversa disposizione di legge o diverso accordo tra le parti.

(2) Una firma elettronica sicura non produce gli effetti giuridici della forma scritta ai sensi del § 886 c.c.g. austriaco nel caso di

1. negozi giuridici rientranti nell'ambito del diritto di famiglia e di successione, i quali richiedano la forma scritta o un requisito di forma più severo,
2. altre dichiarazioni di volontà o negozi giuridici la cui efficacia dipenda da un'autenticazione, da una legalizzazione giudiziaria, da un'autenticazione notarile o da un atto notarile;
3. dichiarazioni di volontà, negozi giuridici o richieste la cui iscrizione nel registro immobiliare, nel registro delle imprese o in un altro registro pubblico richiede un'autenticazione, una legalizzazione giudiziaria, un'autenticazione notarile o un atto notarile;
4. dichiarazioni di garanzia (§ 1346 comma 2 c.c.g. austriaco).

(3) La norma del § 294 c.p.c. sulla presunzione di autenticità del contenuto di una scrittura privata firmata va applicata a documenti elettronici recanti una firma elettronica sicura.

(4) Gli effetti giuridici di cui ai commi 1 e 3 non si producono se viene dimostrato il mancato rispetto dei requisiti di sicurezza previsti nella presente Legge federale e nei relativi regolamenti oppure se viene dimostrata la compromissione delle misure adottate per il rispetto di tali requisiti di sicurezza.

Certificati qualificati

§ 5. (1) Un certificato qualificato deve contenere almeno le seguenti informazioni:

1. il richiamo al fatto che si tratta di un certificato qualificato,
2. il nome non confondibile del certificatore e lo stato in cui ha la propria sede,
3. il nome del firmatario o uno pseudonimo che deve essere indicato come tale,

4. eventualmente su domanda del richiedente, dati su un eventuale potere di rappresentanza o su un altro requisito giuridicamente rilevante del firmatario,
5. i dati per il controllo della firma associati al firmatario,
6. inizio e fine del periodo di validità del certificato,
7. il codice di riconoscimento inequivocabile del certificato,
8. un'eventuale limitazione dell'ambito di impiego del certificato e
9. un'eventuale limitazione del valore delle transazioni effettuabili con il certificato.

(2) Su domanda del richiedente, nel certificato qualificato si possono inserire altre informazioni giuridicamente rilevanti.

(3) Un certificato qualificato deve recare la firma elettronica sicura del certificatore.

Sezione III.

Certificatori

Attività dei certificatori

§ 6. (1) L'inizio dell'attività e l'esercizio dell'attività di certificatore non richiedono un apposito permesso.

(2) Un certificatore deve denunciare senza indugio l'inizio attività all'autorità di vigilanza (§ 13) e produrre all'autorità di vigilanza, al più tardi all'inizio dell'attività oppure in caso di variazione dei propri servizi, un progetto di sicurezza e un progetto di certificazione per ogni servizio di firma e certificazione proposto, incluse le infrastrutture e procedure tecnologiche impiegate.

(3) Un certificatore che propone procedure di firma elettronica sicura deve illustrare nel proprio progetto di sicurezza il rispetto dei requisiti di sicurezza previsti nella presente Legge federale e nei relativi regolamenti.

(4) Un certificatore deve attenersi alle specifiche contenute nel suo progetto di sicurezza e certificazione sia all'inizio dell'attività sia durante l'esercizio dell'attività.

(5) Un certificatore deve segnalare tempestivamente all'autorità di vigilanza qualsiasi circostanza che non consenta più di svolgere l'attività in modo regolare e conforme al progetto di sicurezza e certificazione.

(6) Se il certificatore emette certificati, egli deve esporre nel progetto di sicurezza se ed eventualmente in quale forma intende gestire servizi elenchi e servizi di revoca.

(7) I certificati per i certificatori vanno utilizzati esclusivamente per l'erogazione di servizi di certificazione.

Certificatori che emettono certificati qualificati

§ 7. (1) Un certificatore che emette certificati qualificati deve
1. possedere la necessaria affidabilità per i servizi di firma o certificazione erogati,
2. garantire l'esercizio di un rapido e sicuro servizio elenchi e di un tempestivo e sicuro servizio di revoca,
3. utilizzare nei certificati qualificati e per i servizi elenchi e servizi di revoca un time stamping di qualità garantita, e comunque assicurare la localizzazione temporale dell'emissione e della revoca di un certificato qualificato,
4. verificare attendibilmente, per mezzo di un documento ufficiale d'identità con fotografia, l'identità ed eventualmente particolari requisiti giuridicamente rilevanti della persona per la quale viene emesso un certificato qualificato,
5. servirsi di personale fidato, in possesso delle conoscenze professionali necessarie per i servizi da erogare, specie dotato di capacità in materia di management e know how nel settore della tecnologia delle firme elettroniche e delle procedure di sicurezza, nonché applicare idonee procedure di gestione e management, che siano conformi alle norme riconosciute,

6. disporre di mezzi finanziari sufficienti per rispondere ai requisiti stabiliti nella presente Legge federale e nei relativi regolamenti, nonché cautelarsi per la soddisfazione di eventuali pretese di risarcimento, ad esempio stipulando un'assicurazione di responsabilità civile,
7. registrare per un periodo di tempo adeguato tutte le circostanze di rilievo riguardanti un certificato, eventualmente anche in forma elettronica, onde poter documentare l'avvenuta certificazione specie in caso di procedimenti giudiziari, e
8. adottare misure atte ad impedire la memorizzazione o copiatura da parte del certificatore o di terzi dei dati di cui i firmatari si servono per la generazione della firma.

(2) Un certificatore che emette certificati qualificati deve utilizzare per i servizi di firma e certificazione e per l'emissione e memorizzazione di certificati, sistemi, prodotti e procedure affidabili e protetti contro le contraffazioni, atti a garantire la sicurezza tecnica e crittografica. In particolare deve adottare misure che garantiscano la segretezza dei dati per la generazione della firma, impediscano la falsificazione o contraffazione occulta di certificati qualificati e permettano il richiamo pubblico di questi certificati esclusivamente previa autorizzazione del firmatario. Per l'approntamento dei dati per la generazione della firma e per l'emissione e la memorizzazione di certificati qualificati vanno impiegate infrastrutture e procedure tecnologiche che rispondano ai requisiti specificati al § 18.

(3) I dati per la generazione della firma dei certificatori vanno protetti dall'accesso non autorizzato.

(4) L'esistenza dei presupposti per firme elettroniche sicure, specificati ai commi dall'1 al 3, può essere certificata nell'ambito dell'accreditamento volontario (§ 17).

(5) Se il certificatore propone una procedura di firma elettronica sicura, il fatto che si tratti di una firma elettronica sicura deve comparire nel certificato o in un elenco pubblico, consultabile in qualsiasi momento per via elettronica.

(6) Su richiesta di tribunali o di altre autorità, il certificatore deve provvedere al controllo delle firme sicure basate sui suoi certificati qualificati.

Emissione di certificati qualificati

§ 8. (1) Un certificatore deve accertare con affidabilità l'identità delle persone per le quali va emesso un certificato qualificato, servendosi di un documento ufficiale d'identità con fotografia. Inoltre deve confermare, mediante un certificato qualificato, l'attribuzione a questa persona di determinati dati per il controllo della firma.

(2) La domanda di emissione di un certificato qualificato può essere presentata anche ad un altro ufficio che agisce per incarico del certificatore, il quale ufficio dovrà provvedere all'identificazione del richiedente.

(3) Su domanda del richiedente, il certificatore deve inserire nel certificato qualificato informazioni sul suo potere di rappresentanza o su un altro requisito di rilevanza giuridica, a condizione che queste circostanze vengano documentate attendibilmente al certificatore o ad un altro ufficio (comma 2).

(4) Su domanda del richiedente, un certificatore può indicare nel certificato uno pseudonimo al posto del nome del firmatario, sempre nel rispetto dei princìpi del suo progetto di certificazione. Lo pseudonimo non deve essere sconveniente, né prestarsi palesemente ad essere confuso con nomi o sigle.

Revoca di certificati

§ 9. (1) Un certificatore deve revocare senza indugio un certificato se
1. ne fa richiesta il firmatario o un rappresentato, indicato nel certificato,
2. il certificatore viene a conoscenza della morte del firmatario o comunque del cambiamento di circostanze attestate nel certificato,
3. il certificato è stato ottenuto rendendo informazioni false,
4. il certificatore sospende l'attività e i suoi servizi elenchi e servizi di revoca non vengono rilevati da altri certificatori,
5. l'autorità di vigilanza dispone la revoca del certificato ai sensi del § 14 oppure
6. sussiste il rischio di un uso improprio del certificato.

(2) Se le circostanze di cui al comma 1 non possono essere accertate immediatamente e con sicurezza, il certificatore deve comunque bloccare il certificato senza indugio.

(3) Nel blocco e nella revoca va specificato il momento a partire dal quale acquistano efficacia. Se viene proposto un servizio di revoca, il blocco e la revoca acquistano efficacia contestualmente alla loro registrazione nel rispettivo elenco. Non sono ammessi blocchi o revoche retroattivi. Il firmatario o il suo avente causa va informato prontamente del blocco o della revoca.

(4) Un certificatore deve tenere un elenco pubblico dei certificati qualificati bloccati e revocati, consultabile in qualsiasi momento per via elettronica.

(5) L'autorità di vigilanza deve revocare senza indugio il certificato di un certificatore se:
1. al certificatore viene vietato l'esercizio dell'attività e i suoi servizi elenchi e servizi di revoca non vengono rilevati da un altro certificatore oppure
2. il certificatore sospende l'attività e i suoi servizi elenchi e servizi di revoca non vengono rilevati da un altro certificatore.

Servizi di time stamping

§ 10. Se un certificatore fornisce servizi di time stamping, il suo progetto di sicurezza e certificazione deve contenere dati circostanziati al riguardo. Per la fornitura di servizi di time stamping sicuri vanno utilizzate infrastrutture e procedure tecnologiche che garantiscano la correttezza e l'integrità della localizzazione temporale e rispondano ai requisiti specificati al § 18.

Documentazione

§ 11. (1) Un certificatore deve documentare le misure di sicurezza adottate per il rispetto della presente Legge federale e dei relativi regolamenti, nonché l'emissione e l'eventuale blocco o revoca di certificati. I dati, la loro integrità e il momento del loro inserimento nel sistema di verbalizzazione devono essere verificabili in qualsiasi momento.

(2) Un certificatore deve consegnare la documentazione di cui al comma 1 su richiesta di tribunali o di altre autorità.

Sospensione dell'attività

§ 12. Un certificatore deve segnalare senza indugio la sospensione dell'attività all'autorità di vigilanza. Inoltre deve revocare i certificati validi all'atto della sospensione dell'attività o adoperarsi affinché almeno i suoi servizi elenchi e servizi di revoca vengano rilevati da un altro certificatore. I firmatari vanno informati senza indugio circa la sospensione dell'attività e la revoca o il rilievo dei servizi. Il certificatore deve garantire, anche in caso di revoca dei certificati, la prosecuzione dei servizi di revoca; qualora non facesse fronte a questo obbligo, l'autorità di vigilanza dovrà provvedere alla prosecuzione dei servizi di revoca a spese del certificatore.

Sezione IV.

Vigilanza

Autorità di vigilanza

§ 13. (1) L'autorità di vigilanza è la Commissione di Telekom Control (§ 110 della Legge sulle telecomunicazioni), alla quale compete la vigilanza corrente del rispetto delle disposizioni della presente Legge federale e dei relativi regolamenti.

(2) L'autorità di vigilanza deve in particolare
1. verificare la messa in pratica dei dati contenuti nel progetto di sicurezza e certificazione,
2. controllare l'utilizzazione di idonee infrastrutture e procedure tecnologiche (§ 18) in caso di approntamento di firme elettroniche sicure,
3. accreditare certificatori come specificato al § 17 e
4. porre in atto la sorveglianza organizzativa tramite organismi di convalidazione (§ 19).

(3) L'autorità di vigilanza deve curare un elenco pubblico, consultabile in qualsiasi momento per via elettronica, dei certificati per certificatori validi, bloccati e revocati. Inoltre l'autorità di vigilanza deve curare un elenco pubblico, consultabile in qualsiasi momento per via elettronica, dei certificatori aventi sede nel territorio nazionale, dei certificatori da essa accreditati e dei certificatori di Paesi terzi per i cui certificati risponde un certificatore avente sede nel territorio nazionale, come stabilito al § 24 comma 2 n. 2. Su richiesta, vanno inseriti in questo elenco anche altri certificatori aventi sede all'estero. Nell'elenco dei certificati per i certificatori vanno registrati i loro certificati qualificati per l'erogazione di servizi di certificazione. Questi certificati possono essere emessi anche dall'autorità di vigilanza. Gli elenchi tenuti dall'autorità di vigilanza devono recare la sua firma elettronica sicura. Il certificato dell'autorità di vigilanza va pubblicato nel foglio annunzi ufficiali della Wiener Zeitung.

(4) L'autorità di vigilanza deve prescrivere ai certificatori il pagamento di una commissione, stabilita per decreto, a copertura delle spese risultanti dalla sua attività e dall'intervento di Telekom-Control GmbH. Le commissioni introitate dall'autorità di vigilanza vanno inoltrate a Telekom-Control GmbH o all'organismo di convalidazione in proporzione al rispettivo onere sostenuto.

(5) L'autorità di vigilanza può avvalersi della consulenza di idonee persone o organizzazioni, ad esempio di un organismo di convalidazione (§ 19).

(6) Ai sensi dell'art. 20 comma 2 della Legge costituzionale federale (B-VG), i membri dell'autorità di vigilanza non sono obbligati ad attenersi ad alcuna istruzione nell'esercizio delle loro funzioni. Salvo diversa disposizione di legge, l'autorità di vigilanza deve applicare la Legge generale sul procedimento amministrativo (AVG) del 1991. Essa decide in ultima istanza. È ammesso l'appello alla corte amministrativa.

(7) L'attività dell'autorità di vigilanza prevista nella presente Legge federale va tenuta separata, sotto un profilo organizzativo e finanziario, dall'attività che essa svolge in virtù di altre leggi federali.

Misure di vigilanza

§ 14. (1) L'autorità di vigilanza deve prescrivere ai certificatori l'adozione di misure atte a garantire l'adempimento degli obblighi previsti nella presente Legge federale e nei relativi regolamenti. In particolare l'autorità può vietare ad un certificatore, per intero o in parte, l'utilizzo di infrastrutture e procedure tecnologiche inidonee oppure l'esercizio dell'attività. Inoltre l'autorità può revocare certificati per certificatori o certificati di firmatari oppure disporre ad un certificatore la revoca dei certificati di firmatari.

(2) Salvo l'adozione di provvedimenti più lievi ai sensi del comma 6, ad un certificatore va vietato l'esercizio dell'attività per intero o in parte se

1. il certificatore o il suo personale non possiede l'affidabilità richiesta per l'erogazione dei servizi di firma o certificazione proposti,
2. il certificatore o il suo personale non possiede il know how richiesto,
3. il certificatore non dispone di sufficienti mezzi finanziari,
4. il certificatore non si attiene alle specifiche contenute nel progetto di sicurezza o di certificazione,
5. il certificatore non gestisce o non gestisce correttamente i servizi elenchi o i servizi di revoca oppure non assolve o non assolve adeguatamente l'obbligo di blocco o di revoca (§ 9) oppure
6. non assolve l'obbligo di denuncia specificato al § 6 comma 2.

(3) Salvo l'adozione di provvedimenti più lievi ai sensi del comma 6, ad un certificatore che emette certificati qualificati va altresì vietato l'esercizio dell'attività, per intero o in parte, se mancano gli altri requisiti per l'esercizio di un'attività di questo genere, stabiliti nella presente Legge federale o nei relativi regolamenti.

(4) Salvo l'adozione di provvedimenti più lievi ai sensi del comma 6, ad un certificatore che predispone procedure di firma elettronica sicura va vietato l'esercizio dell'attività, per intero o in parte, se le infrastrutture e procedure tecnologiche impiegate non soddisfano i requisiti di sicurezza specificati al § 18.

(5) Se l'autorità di vigilanza vieta ad un certificatore l'esercizio dell'attività, essa deve provvedere alla revoca dei certificati del certificatore e dei firmatari o disporre che un altro certificatore rilevi i servizi di firma e certificazione erogati o quanto meno i servizi elenchi e di revoca, sempre che i

certificatori interessati convengano sul rilievo. I firmatari vanno tempestivamente informati in ordine al divieto e alla revoca o al rilievo. Il certificatore deve garantire la prosecuzione dei servizi di revoca anche in caso di revoca dei certificati; qualora non facesse fronte a questo obbligo, l'autorità di vigilanza dovrà provvedere alla prosecuzione dei servizi di revoca a spese del certificatore.

(6) L'autorità di vigilanza deve astenersi dal vietare ad un certificatore l'esercizio dell'attività se per garantire il rispetto delle disposizioni della presente Legge federale e dei relativi regolamenti è sufficiente il ricorso a strumenti più lievi. In particolare l'autorità di vigilanza può imporre condizioni o minacciare l'adozione di provvedimenti se entro un termine adeguato non vengono eliminati i vizi rilevati.

Ricorso a Telekom-Control GmbH

§ 15. (1) Per lo svolgimento della sua attività, l'autorità di vigilanza può avvalersi della consulenza di Telekom-Control GmbH (§ 108 TKG).

(2) Telekom-Control GmbH deve in particolare

1. appoggiare l'autorità di vigilanza nell'attività di vigilanza corrente e verificare i prodotti tecnologici, le procedure e gli altri strumenti impiegati nell'ambito dei servizi di firma e certificazione erogati, nonché assicurarsi della qualificazione del personale,
2. registrare i certificatori dopo la denuncia dell'inizio attività,
3. tenere elenchi dei certificati per certificatori, elenchi dei certificatori (§ 13 comma 3) ed un elenco dei certificatori accreditati (§ 17 comma 1),
4. gestire un servizio di revoca in caso di sospensione o divieto dell'attività di un certificatore, sempre che tale servizio non venga rilevato come previsto ai §§ 12 o 14 comma 5,
5. accertare il rispetto dei requisiti richiesti per l'accreditamento volontario (§ 17), previa disposizione dell'autorità di vigilanza,
6. collaborare nell'accertamento dell'equivalenza di verbali di controllo di Paesi terzi ai sensi del § 24 comma 3 e
7. disporre immediatamente il divieto provvisorio dell'esercizio dell'attività del certificatore o l'adozione di misure provvisorie ai sensi del § 14 comma 1 in caso di sospetto fondato del mancato rispetto dei requisiti di sicurezza previsti dalla presente Legge federale o dai relativi regolamenti o su richiesta di un certificatore.

(3) Telekom-Control GmbH deve adottare tutte le misure organizzative atte a garantire l'assolvimento delle proprie funzioni ed appoggiare l'autorità di vigilanza nell'assolvimento delle sue funzioni. Telekom-Control GmbH può avvalersi della consulenza di idonee persone o organizzazioni, ad esempio di un organismo di convalidazione (§ 19). L'assolvimento delle sue funzioni di rilevanza tecnica va definito assieme ad un organismo di convalidazione (§ 19). Nell'ambito della sua attività per l'autorità di vigilanza, il personale di Telekom-Control GmbH è vincolato alle direttive del presidente o del membro indicato nel regolamento interno.

(4) Ferma restando la competenza dei tribunali ordinari, i clienti o i rappresentanti di gruppi d'interesse possono sottoporre a Telekom-Control GmbH controversie o contestazioni non adeguatamente risolte con il certificatore, specie relative alla qualità di un servizio di certificazione. Telekom-Control GmbH deve adoperarsi per il raggiungimento di una soluzione consensuale entro un termine ragionevole. I certificatori hanno l'obbligo di partecipare ad una procedura di questo genere e rendere tutte le informazioni necessarie per la valutazione della situazione di fatto. Telekom-Control GmbH deve fissare direttive per l'esecuzione di tale procedura, le quali vanno pubblicate in forma opportuna.

(5) Il § 13 comma 7, relativo alla separazione organizzativa e finanziaria, va applicato anche all'attività di Telekom-Control GmbH.

Esecuzione dell'attività di vigilanza

§ 16. (1) I certificatori devono consentire agli incaricati dell'autorità di vigilanza l'accesso agli uffici durante gli orari di lavoro, esibire o tenere pronti per la visione i libri e altre registrazioni o documentazioni pertinenti, inclusa la documentazione specificata al § 11, rendere informazioni e fornire loro l'appoggio di cui comunque necessitano. Rimangono impregiudicati i diritti al segreto professionale e la possibilità di avvalersi della facoltà di non rispondere, previsti dalla legge.

(2) Su richiesta, gli organi del servizio di sicurezza pubblico devono appoggiare, per quanto di loro competenza, l'autorità di vigilanza e le persone che agiscono per suo incarico.

(3) L'attività d vigilanza specificata ai commi 1 e 2 va svolta, nei limiti del possibile, avendo riguardo per i coinvolti e senza creare inutile clamore, onde non ledere la sicurezza dei servizi di firma e certificazione.

Accreditamento volontario

§ 17. (1) L'autorità di vigilanza deve accreditare, previa richiesta, i certificatori che propongono procedure di firma elettronica sicura e documentano, prima dell'inizio dell'attività di certificatore accreditato, il rispetto dei requisiti della presente Legge federale e dei relativi regolamenti. Previo assenso dell'autorità di vigilanza, i certificatori accreditati hanno la facoltà di qualificarsi come tali nei rapporti commerciali. Questa qualifica può essere utilizzata in relazione a servizi di firma e certificazione e a prodotti per la firma esclusivamente se vengono soddisfatti i requisiti di sicurezza specificati al § 18. L'autorità di vigilanza deve provvedere all'inserimento dei certificatori accreditati in un elenco pubblico, consultabile in qualsiasi momento per via elettronica.

(2) L'accreditamento volontario di un certificatore va inserito nel certificato qualificato o reso accessibile in altro modo opportuno.

(3) L'autorità di vigilanza deve provvedere al controllo corrente dei certificatori da essa accreditati.

Sezione V.

Requisiti tecnici di sicurezza

Infrastrutture e procedure tecnologiche per firme sicure

§ 18. (1) Per la generazione e la memorizzazione di dati per generazione di una firma e per la generazione di firme sicure vanno impiegate infrastrutture e procedure tecnologiche che permettano l'affidabile individuazione di falsificazioni delle firme e di contraffazioni dei dati firmati e impediscano con altrettanta affidabilità l'utilizzo non autorizzato di dati per la generazione della firma.

(2) Le infrastrutture e procedure tecnologiche utilizzate per la generazione di una firma sicura devono altresì garantire che i dati da firmare non vengano alterati; inoltre devono permettere al firmatario la rappresentazione dei dati firmare prima di avviare l'operazione di firma. L'unicità dei dati per la generazione della firma va garantita con un margine di probabilità ai limiti della certezza; inoltre si deve garantire con sufficiente certezza la non intuibilità di tali dati ed assicurare la loro segretezza.

(3) Per la generazione e la memorizzazione di certificati qualificati vanno impiegate infrastrutture e procedure tecnologiche atte ad impedire la falsificazione e contraffazione dei certificati.

(4) Per il controllo di dati recanti una firma sicura vanno proposte infrastrutture e procedure tecnologiche le quali garantiscano che

1. i dati firmati non sono stati alterati,
2. la firma venga controllata in modo affidabile e l'esito di tale controllo venga correttamente visualizzato,
3. il soggetto che effettua il controllo possa accertare a quali dati si riferisce la firma elettronica,
4. il soggetto che effettua il controllo possa accertare a quale soggetto è associata la firma elettronica, con visualizzazione di un eventuale pseudonimo; e
5. si possa riconoscere se i dati firmati hanno subìto alterazioni rilevanti per la sicurezza.

(5) Le infrastruttura e procedure tecnologiche per la generazione di firme sicure devono essere controllate adeguatamente e correntemente in base allo stato della tecnica. Il rispetto dei requisiti di sicurezza deve essere certificato da un organismo di convalidazione (§ 19).

Organismo di convalidazione

§ 19. (1) I compiti assegnati ad un organismo di convalidazione in virtù della presente Legge federale e dei relativi regolamenti, possono essere assolti esclusivamente da un'organizzazione in possesso dei necessari requisiti.

(2) Un'organizzazione è idonea all'assolvimento dei compiti assegnati ad un organismo di convalidazione se

1. possiede l'affidabilità richiesta,
2. occupa personale affidabile che sia in possesso delle conoscenze professionali, esperienze e qualificazioni necessarie per questi compiti, specie di conoscenze nei settori delle firme elettroniche, procedure di sicurezza, crittografia, tecnologie di comunicazione, schede a microprocessore, nonché per la valutazione tecnica di tali componenti,
3. dispone di adeguate strutture e mezzi tecnici e di un'adeguata potenzialità economica, e
4. garantisce la necessaria autonomia, imparzialità e obiettività.

(3) Il Cancelliere federale deve stabilire per decreto, d'intesa con il Ministro federale della giustizia, che una organizzazione è in possesso dei requisiti per operare come organismo di convalidazione. Un tale decreto può essere emanato esclusivamente su richiesta dell'organizzazione in questione. L'idoneità può essere decretata esclusivamente se dagli statuti o dall'atto costitutivo, dall'organizzazione e dal progetto di sicurezza e finanziamento risulta che l'organizzazione soddisfa i requisiti di cui al comma 2.

(4) Per l'assolvimento dei compiti affidatigli in virtù della presente Legge e dei relativi regolamenti, un organismo di convalidazione può chiedere ad altre organizzazioni o uffici la stesura di verbali di controllo di infrastrutture e procedure tecnologiche.

Sezione VI.

Diritti ed obblighi degli utilizzatori

Obblighi generali d'informazione dei certificatori

§ 20. (1) Prima della stipula del contratto, il certificatore deve informare il richiedente circa il contenuto del progetto di sicurezza e certificazione, in modo chiaro e generalmente comprensibile, per iscritto o mediante un supporto dati incancellabile. All'atto dell'emissione di un certificato qualificato, il certificatore deve inoltre rendere note le condizioni per l'utilizzo del certificato, quali ad esempio le limitazioni dell'ambito d'impiego e del valore delle transazioni; inoltre deve evidenziare un eventuale accreditamento volontario (§ 17) e le procedure speciali per il regolamento delle controversie.

(2) I dati riportati al comma 1 vanno resi accessibili anche su richiesta di terzi che dimostrino di averne un legittimo interesse.

(3) Un certificatore deve inoltre comunicare al richiedente quali sono le infrastrutture e procedure tecnologiche idonee per il metodo di firma impiegato, ed eventualmente quali infrastrutture e procedure tecnologiche ed altre misure soddisfano i requisiti per la generazione ed il controllo di firme sicure. Inoltre il richiedente va informato sui possibili effetti giuridici della procedura di firma da lui impiegata, sugli obblighi del firmatario e sulla responsabilità speciale del certificatore. Il richiedente va altresì informato in ordine alla necessità e alle modalità di apposizione di una nuova firma elettronica prima che il grado di sicurezza della firma esistente diminuisca per decorrenza dei tempi.

Obblighi del firmatario

§ 21. Il firmatario deve conservare con cura i dati per la generazione della firma, impedire per quanto possibile l'accesso a tali dati ed astenersi dalla loro divulgazione. Il firmatario deve chiedere la revoca del certificato in caso di smarrimento dei dati per la generazione della firma, di sospetto di una loro compromissione oppure di cambiamenti delle circostanze attestate nel certificato.

Tutela dei dati

§ 22. (1) Un certificatore deve utilizzare esclusivamente quei dati personali di cui necessita per l'erogazione dei servizi proposti. Questi dati vanno acquisiti direttamente presso il soggetto interessato o presso un terzo, ma con l'espressa autorizzazione dell'interessato.

(2) Qualora venga impiegato uno pseudonimo, il certificatore è tenuto a trasmettere i dati relativi all'identità del firmatario purché venga dimostrato il prevalere di un legittimo interesse all'accertamento dell'identità ai sensi del § 8 comma 1 n. 4 e comma 3 della Legge sulla tutela dei dati. Questa trasmissione va documentata.

(3) Rimangono impregiudicati gli obblighi d'informazione e cooperazione del certificatore verso i tribunali ed altre autorità.

Responsabilità dei certificatori

§ 23. (1) Un certificatore che emette un certificato qualificato o che risponde per un certificato di questo genere ai sensi del § 24 comma 2 n. 2, si rende responsabile verso ogni soggetto che fa affidamento sul certificato

1. per la correttezza di tutti i dati contenuti nel certificato qualificato all'atto della sua emissione,
2. per il fatto che, all'atto dell'emissione del certificato qualificato, il firmatario indicato nel certificato era in possesso di quei dati per la generazione della firma che corrispondono ai dati per il controllo della firma a loro volta indicati nel certificato,
3. per la complementarietà tra i dati per la generazione della firma e i relativi dati per il controllo della firma in caso di impiego dei prodotti e delle procedure forniti o indicati come idonei dal certificatore,
4. per la revoca tempestiva del certificato, in presenza delle necessarie condizioni, e per la disponibilità dei servizi di revoca e
5. per il rispetto dei requisiti specificati al § 7 e l'impiego di infrastrutture e procedure tecnologiche per la generazione e la memorizzazione di dati per la generazione della firma conformi al § 18.

(2) Un certificatore che propone procedure di firma elettronica sicura risponde inoltre per l'impiego esclusivo di infrastrutture e procedure tecnologiche conformi al § 18 per i prodotti, procedure o altri strumenti da lui predisposti o indicati come idonei per la generazione di firme elettroniche e per la rappresentazione dei dati da firmare.

(3) Il certificatore non risponde nel caso in cui dimostri che l'inadempimento degli obblighi di cui ai commi 1 e 2 non è imputabile a colpa propria e dei propri collaboratori. Qualora la parte lesa sia in grado di dimostrare come probabile che gli obblighi di cui ai commi 1 e 2 sono stati violati o che le misure adottate per il rispetto dei requisiti di sicurezza della presente Legge federale e dei relativi regolamenti sono state compromesse, si dovrà presumere che il danno dipenda da queste cause. Questa presunzione viene oppugnata se il certificatore è in grado di dimostrare la probabilità che il danno non sia stato causato da una violazione degli obblighi o compromissione delle misure citate nella seconda proposizione.

(4) Se un certificato qualificato contiene una limitazione dell'ambito di applicazione, il certificatore non risponde per danni risultanti da un uso difforme del certificato. Se un certificato qualificato contiene un determinato valore limite delle transazioni effettuabili, il certificatore non risponde per danni risultanti da un superamento di tale valore.

(5) La responsabilità del certificatore specificata ai commi 1 - 3, non può essere né esclusa né limitata a priori.

(6) Rimangono impregiudicate le norme del c.c.g. austriaco e altre norme di legge che stabiliscono un diverso risarcimento del danno o la responsabilità di persone diverse da quelle indicate nella presente Legge federale.

Sezione VII.

Riconoscimento di certificati stranieri

Riconoscimento

§ 24. (1) Sono equiparati a certificati nazionali i certificati emessi da un certificatore avente sede nella Comunità Europea e la cui validità può essere verificata nel territorio nazionale. Certificati qualificati di tali certificatori producono i medesimi effetti giuridici dei certificati qualificati nazionali.

(2) Vengono riconosciuti nel territorio nazionale i certificati emessi da un certificatore avente sede in un Paese terzo e la cui validità può essere verificata nel territorio nazionale. Certificati qualificati vengono equiparati giuridicamente a certificati qualificati nazionali se

1. il certificatore soddisfa i requisiti specificati al § 7 ed è accreditato in un sistema di accreditamento volontario di uno stato membro dell'Unione europea,
2. un certificatore avente sede nella Comunità Europea che soddisfa i requisiti specificati al § 7, risponde giuridicamente per il certificato oppure
3. il certificato è riconosciuto come certificato qualificato oppure il certificatore è riconosciuto come emittente di certificati qualificati nell'ambito di un accordo bilaterale o multilaterale tra la Comunità Europea da un lato e Paesi terzi o organizzazioni internazionali dall'altro.

(3) Se in uno stato membro dell'Unione Europea o in un Paese terzo è stato istituito un organismo riconosciuto dallo stato per la dimostrazione dei requisiti di sicurezza per firme elettroniche sicure, gli attestati di questo organismo relativi al rispetto dei requisiti di sicurezza per la generazione di firme elettroniche sicure vengono equiparati agli attestati di un organismo di convalidazione (§ 19) purché l'autorità di vigilanza accerti che i requisiti tecnici, i controlli e le procedure di controllo che stanno alla base delle valutazioni di questi organismi sono equivalenti a quelli dell'organismo di convalidazione.

Sezione VIII.

Disposizioni finali

Regolamento sulla firma elettronica

§ 25. Il Cancelliere federale d'intesa con il Ministro federale della giustizia ha emanato per decreto i regolamenti che, in base allo stato della scienza e della tecnica, sono necessari per l'attuazione della presente Legge federale, aventi come oggetto:

1. la fissazione e prescrizione di commissioni forfettarie a copertura delle spese per le prestazioni dell'autorità di vigilanza e di Telekom-Control GmbH,
2. la fissazione di sufficienti mezzi finanziari per il rispetto dei requisiti stabiliti nella presente Legge federale e nei relativi regolamenti e dei mezzi finanziari a copertura del rischio di responsabilità dei certificatori, ed in particolare la fissazione di un massimale minimo per l'assicurazione di responsabilità civile,
3. l'affidabilità del certificatore e del suo personale (§§ 7 comma 1 e 14 comma 2),
4. la precisazione dei requisiti delle infrastrutture e procedure tecnologiche, dei prodotti tecnologici e di altri strumenti per l'applicazione dei §§ 7 commi 2, 10 e 18, dei requisiti per il controllo delle infrastrutture e procedure tecnologiche ai sensi del § 18 e per il rilascio della conferma del rispetto di questi requisiti,
5. il periodo di assunzione dei servizi di revoca da parte dell'autorità di vigilanza (§ 12 e § 14 comma 5),
6. gli ambiti di applicazione, i requisiti e le tolleranze di servizi di time stamping sicuri,
7. il periodo di validità e il rinnovo di certificati qualificati e il periodo e la procedura in base ai quali si dovrebbe apporre una nuova firma elettronica (post-firma),
8. la forma, la rappresentazione e la disponibilità del progetto di certificazione (ad esempio testo in chiaro),
9. il periodo di conservazione di una documentazione (§ 11) e
10. il tipo e la forma dell'identificazione di certificatori accreditati.

Disposizioni sulle sanzioni amministrative

§ 26. (1) Incorre in una contravvenzione amministrativa sanzionabile con un'ammenda fino a ATS 56.000 chi utilizza abusivamente dati altrui per la generazione della firma all'insaputa e senza la volontà dell'avente diritto.

(2) Un certificatore incorre in una contravvenzione amministrativa sanzionabile con un'ammenda fino a ATS 112.000 se:

1. in violazione del § 9 comma 1 non adempie al proprio obbligo di revoca,
2. in violazione del § 11 non adempie al proprio obbligo di documentazione,
3. in violazione del § 16 comma 1 non permette la presa in visione dei libri, altre registrazioni o documentazioni o non fornisce le dovute informazioni,
4. in violazione del § 20 commi 1 e 3 non informa il soggetto che richiede un certificato.

(3) Un certificatore incorre in una contravvenzione amministrativa sanzionabile con un'ammenda fino a ATS 224.000 se

1. in violazione del § 6 comma 2 non denuncia l'inizio attività o non produce il progetto di sicurezza o certificazione,
2. in violazione del § 6 comma 5 non denuncia all'autorità di vigilanza qualsiasi circostanza che non gli consenta più di svolgere l'attività in modo regolare e conforme al progetto di sicurezza e certificazione,
3. in violazione del § 7 comma 1 n. 2 non gestisce un idoneo servizio di revoca o un idoneo servizio elenchi,
4. in violazione del § 7 comma 1 n. 8 non adotta misure atte ad impedire che il certificatore o terzi possano memorizzare o copiare i dati per la generazione della firma dei firmatari,
5. in violazione del § 18 non utilizza, predispone o indica idonee infrastrutture e procedure tecnologiche per firme elettroniche sicure, oppure
6. malgrado il divieto da parte dell'autorità di vigilanza (§ 14 commi 2-4), continua ad esercitare l'attività.

(4) Non si è in presenza di una contravvenzione amministrativa ai sensi dei commi 1-3, se il fatto costituisce la fattispecie di un reato rientrante nella sfera di competenza dei tribunali oppure è soggetto a pene più severe in virtù di altre disposizioni in materia di sanzioni amministrative.

(5) Nella sentenza si può dichiarare la confisca degli oggetti con i quali è stato commesso il reato.

Entrata in vigore e rinvii

§ 27. (1) La presente Legge federale entra in vigore il 1° gennaio 2000.

(2) Se la presente Legge federale contiene rinvii a disposizioni di altre Leggi federali, queste ultime vanno applicate nella loro versione in vigore.

Esecuzione

§ 28. L'esecuzione della presente Legge federale è affidata

1. per quanto attiene i §§ 3, 4 e 23 al Ministro federale della giustizia
2. per quanto attiene i §§ dal 13 al 17 al Ministro federale della scienza e dei trasporti,
3. per quanto attiene i §§ 22 e 26 al Cancelliere federale,
4. per quanto attiene i §§ 7 comma 1 n. 6 e 13 comma 4 al Cancelliere federale d'intesa con il Ministro federale della giustizia ed il Ministro federale delle finanze e
5. per quanto attiene le restanti disposizioni al Cancelliere federale d'intesa con il Ministro federale della giustizia.

Klestil

Klima

STAMPA: PRINT MEDIA AUSTRIA AG (EX ÖSTERREICHISCHE STAATSDRUCKEREI AG)