Ordinanza sui servizi di certificazione elettronica (OSCert)

del 12 aprile 2000

Il Consiglio federale svizzero,

visti gli articoli 28, 62 e 64 della legge federale del 30 aprile 1997[1] sulle telecomunicazioni (LTC);
visti gli articoli 10, 14 e 15 della legge federale del 6 ottobre 1995[2] sugli ostacoli tecnici al commercio (LOTC),

ordina:

Capitolo 1: Disposizioni generali

Art. 1 Oggetto e scopo

[1] La presente ordinanza definisce, sotto forma di regolamentazione a carattere sperimentale, le condizioni alle quali i prestatori di servizi di certificazione hanno la facoltà di chiedere di essere riconosciuti e disciplina le loro attività nel settore dei certificati elettronici.

[2] È volta a promuovere la fornitura di servizi di certificazione elettronica sicuri ad un vasto pubblico, promuovere l'utilizzo e il riconoscimento giuridico delle firme digitali e permettere il riconoscimento internazionale dei prestatori di servizi di certificazione e delle loro prestazioni.

[3] Sono fatte salve le disposizioni di diritto privato relative alla conclusione dei contratti e alla rappresentanza delle persone giuridiche.

Art. 2 Definizioni

Nella presente ordinanza s'intendono per:

a. *prestatore di servizi di certificazione*: una persona fisica o giuridica o un'unità dell'amministrazione federale, cantonale o comunale che certifica informazioni in un ambito elettronico e che rilascia a tal fine certificati elettronici;

b. *certificato elettronico*: un insieme di dati elettronici che stabiliscono il legame tra una chiave pubblica e una persona fisica o giuridica o un'unità amministrativa, autenticati mediante la firma digitale di un prestatore di servizi di certificazione;

RS **784.103**
1 RS **784.10**
2 RS **946.51**

c. *chiave privata*: una chiave crittografica tenuta segreta;

d. *chiave pubblica:* una chiave crittografica che corrisponde ad una chiave privata ed è a disposizione del pubblico;

e. *chiave crittografica:* un parametro utilizzato con un algoritmo matematico per trasformare, convalidare, autenticare, cifrare o decifrare dati;

f. *firma elettronica*: un codice elettronico allegato oppure connesso tramite associazione logica a dati elettronici e cifrato mediante una chiave privata, che permette di verificare, dopo il deciframento mediante la chiave pubblica corrispondente, che i dati provengono effettivamente dal titolare della chiave privata e che non sono stati modificati dopo essere stati firmati;

g. *organismo di riconoscimento*: un organismo di certificazione accreditato ai sensi dell'ordinanza del 17 giugno 1996[3] sull'accreditamento e la designazione che procede alla valutazione e al riconoscimento dei prestatori di servizi di certificazione.

Capitolo 2: Riconoscimento dei prestatori di servizi di certificazione

Art. 3 Riconoscimento

1 Possono essere riconosciuti i prestatori di servizi di certificazione che sono in grado di rilasciare e gestire i certificati elettronici conformemente alle esigenze della presente ordinanza.

2 Gli organismi di riconoscimento accreditati nell'ambito della presente ordinanza sono competenti per riconoscere i prestatori di servizi di certificazione.

3 Se non esiste alcun organismo di riconoscimento, il Servizio d'accreditamento svizzero (SAS) dell'Ufficio federale di metrologia riconosce i prestatori di servizi di certificazione.

Art. 4 Condizioni per il riconoscimento

1 Per essere riconosciuti, i prestatori di servizi di certificazione devono soddisfare le seguenti condizioni:

a. essere iscritti nel registro di commercio o fare parte di un'unità amministrativa della Confederazione, di un Cantone o di un Comune;

b. impiegare personale con le conoscenze, l'esperienza e le qualifiche necessarie;

c. utilizzare sistemi e prodotti informatici affidabili;

d. disporre di risorse e garanzie finanziarie sufficienti;

3 RS **946.512**

e. stipulare le assicurazioni necessarie per coprire i rischi della loro responsabilità civile e le spese derivanti dalle misure previste nell'articolo 15 capoversi 2 e 3;

f. impegnarsi nelle loro condizioni generali a rispondere anche per i danni provocati a terzi da un certificato elettronico difettoso oppure dall'inadempimento di obblighi sulla pubblicazione, a meno che provino di non avere colpa;

g. garantire l'osservanza del diritto applicabile in materia, segnatamente della presente ordinanza e delle sue disposizioni d'esecuzione.

2 Le condizioni sono precisate nelle disposizioni d'esecuzione.

Art. 5 Lista dei prestatori di servizi di certificazione riconosciuti

1 Gli organismi di riconoscimento annunciano al SAS i prestatori di servizi di certificazione che riconoscono.

2 Il SAS tiene a disposizione del pubblico la lista dei prestatori di servizi di certificazione riconosciuti.

3 Ogni prestatore di servizi di certificazione riconosciuto pubblica la lista di tutti gli altri prestatori di servizi di certificazione riconosciuti come pure la loro chiave pubblica. Egli autentica la lista apponendovi la sua firma digitale. Le altre modalità di pubblicazione sono disciplinate nelle disposizioni d'esecuzione.

Capitolo 3: Esigenze fondamentali

Sezione 1: Creazione e utilizzo delle chiavi crittografiche

Art. 6

Le questioni legate alla creazione delle chiavi crittografiche che possono essere oggetto di certificati elettronici ai sensi della presente ordinanza come pure quelle legate alla creazione e alla verifica della firma elettronica sono disciplinate nelle disposizioni d'esecuzione. Esse intendono garantire un elevato livello di sicurezza in funzione del progresso tecnico.

Sezione 2: Certificati elettronici

Art. 7

1 Ogni certificato elettronico rilasciato ai sensi della presente ordinanza deve contenere almeno le seguenti informazioni:

a. il suo numero di serie;

b. la menzione che è stato rilasciato ai sensi della presente ordinanza;

c. la menzione d'eventuali limiti fissati per il suo utilizzo;

d. il nome del titolare della chiave pubblica certificata come pure la menzione che si tratta di una persona fisica, di una persona giuridica, di un'unità amministrativa oppure, se del caso, di uno pseudonimo;

e. la chiave pubblica certificata;

f. la durata di validità;

g. il nome e la firma digitale del prestatore di servizi di certificazione che lo rilascia.

2 Il formato dei certificati è disciplinato nelle disposizioni d'esecuzione.

Sezione 3: Prestatori di servizi di certificazione

Art. 8 Rilascio di certificati elettronici

1 I prestatori di servizi di certificazione riconosciuti devono esigere che i richiedenti un certificato elettronico provino la loro identità e i loro poteri presentando personalmente i seguenti documenti:

a. per le persone fisiche: una carta d'identità o un passaporto;

b. per le persone che agiscono per conto di unità amministrative: una procura e una carta d'identità o un passaporto;

c. per le persone giuridiche: un estratto del registro di commercio e la carta d'identità o il passaporto delle persone abilitate ad agire in loro nome.

2 Qualora una persona o un'unità amministrativa identificata conformemente al capoverso 1 da meno di dieci anni richieda un nuovo certificato elettronico, i prestatori di servizi di certificazione riconosciuti possono accettare una richiesta munita della firma digitale apposta mediante la chiave privata che corrisponde alla chiave pubblica oggetto del certificato da rinnovare.

3 Su richiesta, essi fanno figurare sul certificato elettronico uno pseudonimo al posto del nome del titolare della chiave pubblica certificata. L'identità di quest'ultimo deve essere stabilita conformemente ai capoversi 1 e 2.

Art. 9 Obbligo d'informare

1 I prestatori di servizi di certificazione riconosciuti devono tenere a disposizione del pubblico le loro condizioni generali del contratto come pure le informazioni relative alla loro politica di certificazione.

2 Al più tardi al momento del rilascio dei certificati elettronici, essi devono informare i propri clienti sulle conseguenze della divulgazione o della perdita della loro chiave privata. Essi devono indicare loro le misure appropriate per mantenere segreta la propria chiave.

Art. 10 Conservazione delle chiavi private

I prestatori di servizi di certificazione riconosciuti non possono conservare copie delle chiavi private dei loro clienti.

Art. 11 Annullamento dei certificati elettronici

1 I prestatori di servizi di certificazione riconosciuti annullano immediatamente i certificati elettronici su richiesta dei loro titolari.

2 I prestatori di servizi di certificazione riconosciuti devono verificare la legittimazione di chi richiede l'annullamento. Tale esigenza è considerata soddisfatta quando la richiesta è munita della firma digitale apposta mediante la chiave privata che corrisponde alla chiave pubblica oggetto del certificato da annullare.

3 Essi sono tenuti ad annullare immediatamente i certificati elettronici che risultano essere stati ottenuti in modo fraudolento o che non permettono più di garantire il legame tra una persona o un'unità amministrativa e una chiave pubblica.

4 Essi possono sospendere provvisoriamente i certificati elettronici per una durata massima di tre giorni. Trascorso questo lasso di tempo, annullano definitivamente i certificati o ne ristabiliscono la validità. Nel primo caso, l'annullamento è efficace dal momento in cui il certificato è stato sospeso; nel secondo caso, la sospensione non ha effetto sulla validità del certificato.

5 I prestatori di servizi di certificazione riconosciuti informano senza indugio i titolari dei certificati elettronici dell'annullamento o della sospensione di questi ultimi.

Art. 12 Elenco dei certificati elettronici e lista dei certificati annullati o sospesi

1 I prestatori di servizi di certificazione riconosciuti tengono un elenco dei certificati elettronici che rilasciano, nel quale i loro clienti possono fare iscrivere i propri certificati elettronici.

2 Devono tenere una lista aggiornata di tutti i certificati annullati o sospesi, anche se non sono stati iscritti nell'elenco. Questa lista menziona unicamente il numero di serie del certificato elettronico, la menzione che è annullato o sospeso, come pure la data e l'ora dell'annullamento o della sospensione. La lista viene autenticata dalla firma digitale del prestatore di servizi di certificazione riconosciuto.

3 I prestatori di servizi di certificazione riconosciuti devono garantire costantemente ai terzi l'accesso online all'elenco dei certificati elettronici e alla lista dei certificati annullati o sospesi, senza ulteriori spese se non quelle di utilizzazione dei mezzi di telecomunicazione pubblici.

4 Le modalità di tenuta degli elenchi di certificati elettronici e delle liste di certificati annullati o sospesi come pure quelle di accesso agli elenchi e alle liste sono disciplinate nelle disposizioni d'esecuzione.

Art. 13 Conservazione dei certificati elettronici

1 I prestatori di servizi di certificazione riconosciuti devono conservare i certificati elettronici scaduti o annullati come pure le liste dei certificati annullati e permettere la loro consultazione per un periodo di almeno undici anni a partire dalla data di scadenza o d'annullamento dei certificati.

2 Durante i primi sei anni, la consultazione deve essere garantita in ogni momento online senza ulteriori spese se non quelle di utilizzazione dei mezzi di telecomunicazione pubblici.

Art. 14 Giornale delle attività

1 I prestatori di servizi di certificazione riconosciuti annotano in un giornale le attività relative al rilascio, all'annullamento e alla sospensione dei certificati elettronici.

2 Essi conservano le iscrizioni nel giornale come pure i documenti giustificativi corrispondenti almeno per il lasso di tempo durante il quale devono conservare l'ultimo certificato rinnovato giusta l'articolo 8 capoverso 2.

Art. 15 Cessazione d'attività

1 I prestatori di servizi di certificazione riconosciuti annunciano al SAS con 30 giorni di preavviso la cessazione delle loro attività. Essi annunciano senza indugio al SAS il ricevimento di una comminatoria di fallimento.

2 In caso di cessazione volontaria d'attività, i prestatori di servizi di certificazione riconosciuti devono annullare i certificati elettronici non scaduti che hanno rilasciato. Il SAS incarica un altro prestatore di servizi di certificazione riconosciuto di tenere la lista dei certificati annullati e di conservare i certificati scaduti o annullati, il giornale delle attività e i documenti giustificativi corrispondenti.

3 In caso di fallimento di un prestatore di servizi di certificazione riconosciuto, il SAS incarica un altro prestatore di servizi di certificazione riconosciuto di annullare i certificati elettronici non scaduti che ha rilasciato, di tenere la lista dei certificati annullati e di conservare i certificati scaduti o annullati, il giornale delle attività e i documenti giustificativi corrispondenti.

Art. 16 Protezione dei dati

1 I prestatori di servizi di certificazione riconosciuti possono raccogliere ed elaborare unicamente i dati personali necessari all'esecuzione dei propri compiti.

2 Per il rimanente, è applicabile la legislazione sulla protezione dei dati.

Capitolo 4: Sorveglianza sui prestatori di servizi di certificazione riconosciuti

Art. 17

1 La sorveglianza sui prestatori di servizi di certificazione riconosciuti è garantita da organismi di riconoscimento secondo le regole del diritto d'accreditamento.

2 L'organismo di riconoscimento deve annunciare immediatamente al SAS la revoca del riconoscimento di un prestatore di servizi di certificazione. È applicabile l'articolo 15 capoverso 3.

Capitolo 5: Riconoscimento dei prestatori di servizi di certificazione stranieri

Art. 18

Il SAS tiene a disposizione del pubblico la lista dei prestatori di servizi di certificazione stranieri riconosciuti nell'ambito degli accordi internazionali conclusi dal Consiglio federale in virtù dell'articolo 14 LOTC.

Capitolo 6: Attestazione di conformità di una firma digitale alla presente ordinanza

Art. 19

1 Su richiesta e dietro pagamento di una tassa amministrativa, il SAS attesta per scritto che la firma digitale figurante su un documento elettronico è stata apposta mediante la chiave privata che corrisponde a una chiave pubblica oggetto di un certificato elettronico rilasciato da un prestatore di servizi di certificazione riconosciuto e che tale certificato era valido in un determinato momento.

2 Il Dipartimento federale di giustizia e polizia fissa l'ammontare della tassa amministrativa.

3 Gli attestati di cui al capoverso 1 possono anche essere forniti da altri organismi nella misura in cui quest'ultimi adempiono le condizioni richieste.

Capitolo 7: Disposizioni finali

Art. 20 Esecuzione

L'Ufficio federale delle comunicazioni emana le disposizioni d'esecuzione previste dalla presente ordinanza, in collaborazione con l'Organo strategia informatica della Confederazione e il SAS. Esso tiene conto delle norme e delle disposizioni internazionali del settore.

Art. 21 Entrata in vigore e durata di validità

1 La presente ordinanza entra in vigore il 1° maggio 2000.

2 Ha effetto fino all'entrata in vigore di una legislazione in materia, ma al più tardi sino al 31 dicembre 2009.

12 aprile 2000 In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Adolf Ogi
La cancelliera della Confederazione, Annemarie Huber-Hotz

2048