Linee guida per l'utilizzo

della Firma Digitale

Versione 1.1 – maggio 2004

1. Scopo e destinatari del documento *3*

2. Definizioni *4*

3. Struttura del documento *6*

4. Introduzione alle sottoscrizioni informatiche *7*

5. Utilizzo della firma digitale *8*

6. La firma digitale e la direttiva europea sulle firme elettroniche *9*

6.1 Firme "leggere" e firme "forti" **9**

7. La diffusione della "firma digitale" in Europa *11*

8. Il valore legale della firma digitale in Italia *12*

9. Dove e come dotarsi di firma digitale *13*

9.1 Il kit di firma digitale ed i costi **13**

9.2 I Cittadini **13**

9.3 Le Imprese **13**

9.4 Le pubbliche Amministrazioni **14**

10. La procedura di firma digitale *15*

10.1 Firma digitale di un singolo documento **15**

10.2 Firma digitale con procedure automatiche **15**

11. La procedura di verifica *17*

11.1 Esempio di verifica **18**

11.2 Procedure automatiche **20**

12. Lo strumento "firma digitale" integrato nel processo di e-government *21*

13. Appendice: la Direttiva Europea 1999/93/CE *22*

1. Scopo e destinatari del documento

Questo breve documento ha lo scopo di chiarire cosa sia la firma digitale, le differenze sostanziali fra le varie tipologie di firme elettroniche, le modalità con cui è possibile dotarsi di un dispositivo di firma digitale, come effettuare la verifica di una firma digitale e gli utilizzi pratici di questo strumento.
Il documento si rivolge ai cittadini, alle imprese ed alle pubbliche amministrazioni che intendono dotarsi dei dispositivi di firma necessari per sottoscrivere con firma digitale i documenti informatici.

2. Definizioni

Certificato qualificato	Insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Chiave privata	La chiave della coppia utilizzata nel processo di sottoscrizione di un documento informatico
Chiave pubblica	La chiave della coppia utilizzata da chiunque esegua la verifica di una firma digitale
Dispositivo di firma	Insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici
Documento informatico	E' costituito da qualunque oggetto informatico (file) che contenga atti, fatti o dati giuridicamente rilevanti
Firma digitale	E' un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
Firma elettronica avanzata	Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
Firma elettronica qualificata	La firma elettronica avanzata che sia basata su un certificato qualificato, creata mediante un dispositivo sicuro per la creazione della firma
Soggetto giuridico	Impresa, azienda, società; qualunque soggetto dotato di partita IVA
SSCD	Acronimo inglese (Secure Signature Creation Device) di "dispositivo sicuro per la creazione della firma". E' un dispositivo che soddisfa particolari requisiti di sicurezza. I più utilizzati sono costituiti da smartcard.
Titolare	Il soggetto cui sono attribuite le firme digitali generate attraverso una determinata chiave associata ad un determinato certificato

Norme di riferimento

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445
Direttiva europea 1999/93/CE sulle firme elettroniche

Decreto legislativo 23 gennaio 2002, n. 10
Decreto del Presidente della Repubblica 7 aprile 2003, n. 137
Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004

3. Struttura del documento

Il documento è strutturato per argomenti indipendenti. Lo scopo è quello di consentire anche la lettura delle sole sezioni di interesse. La seguente tabella ha lo scopo di indirizzare coloro che intendono leggere esclusivamente gli argomenti di loro interesse nell'individuazione degli stessi.
Per ogni argomento è quindi suggerito, dipendentemente dalla tipologia del lettore, il grado di attinenza alle esigenze informative peculiari.

Argomenti	**Cittadini**	**Aziende**	**PA**
Introduzione alle firme elettroniche	C	C	C
Utilizzo della firma digitale	C	C	C
Il quadro normativo di riferimento	A	C	FC
La Firma Digitale e la direttiva Europea sulle firme elettroniche	A	C	C
La Firma Digitale in Europa: diffusione e valore legale	A	A	A
Il valore legale della Firma Digitale in Italia	FC	FC	FC
Dove e come dotarsi di firma digitale	FC	FC	FC
La procedura di Firma Digitale	FC	FC	FC
Firma digitale di un singolo documento	FC	FC	FC
Firma digitale con procedure automatiche	A	A	C
La procedura di verifica	FC	FC	FC
Verifica su client	FC	FC	FC
Verifica su server	C	A	A
Procedure automatiche	A	A	FC
Lo strumento "Firma Digitale" nel processo di e-Government	A	A	A

FC= Lettura fortemente consigliata. **C**= Lettura consigliata. **A**= Lettura di approfondimento

4. Introduzione alle sottoscrizioni informatiche

A partire del 1997, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma digitale. La pubblicazione della Direttiva Europea 1999/93/CE (Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures), nel gennaio del 2000, ha dato ulteriori impulsi al processo legislativo, imponendo un quadro comune agli Stati dell'Unione Europea. Il processo legislativo ha anche fornito delle indicazioni sulle tecnologie da impiegare per ottenere delle firme digitali che possano ritenersi equivalenti a quelle autografe. La struttura normativa dettata dal legislatore comunitario ha introdotto differenti sottoscrizioni o, più correttamente, differenti livelli di sottoscrizione. Nel linguaggio corrente, quindi, hanno iniziato a essere utilizzati i termini firma "debole" o "leggera" e firma "forte" o "pesante". Non è obiettivo di queste Linee Guida approfondire questi concetti, ma senz'altro è opportuno chiarire cosa sono queste firme e quale è la loro efficacia giuridica. Un breve approfondimento giuridico è sviluppato nel paragrafo 6 mentre nel seguito del paragrafo vengono presentati i principali aspetti tecnici.

Dal punto di vista tecnico e realizzativo è ben definita la firma "forte", ovvero quella che il legislatore definisce firma digitale. Essa è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.

L'altra tipologia di firma è la parte complementare. Tutto ciò che non risponde anche in minima parte a quanto appena descritto, ma è compatibile con la definizione giuridica di firma elettronica presentata nella tabella delle definizioni, è un firma "leggera".
Ovviamente l'efficacia giuridica delle due firme è diversa. La firma digitale è equivalente a una sottoscrizione autografa. Le altre potrebbero non esserlo: vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza.

Come ulteriore garanzia per la pubblica amministrazione, che è obbligata ad accettare i documenti firmati digitalmente, i certificatori che intendono rilasciare certificati digitali validi per le sottoscrizioni di istanze e dichiarazioni inviate per via telematica alla pubblica amministrazione stessa, possono dimostrare di possedere particolari e comunque superiori caratteristiche di qualità e sicurezza e ottenere quindi la qualifica di "certificatore accreditato". Tale qualifica è sotto il controllo ed è garantita, in Italia, dallo Stato.

Concludendo, possiamo dire che nell'utilizzo del documento informatico, quando si ha la necessità di una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale.
Negli altri casi possiamo tranquillamente affermare che più che di un processo di firma si tratta di un processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria.

Da quanto esposto si può dedurre che nella pubblica amministrazione l'espressione del potere di firma nel documento informatico da parte del funzionario che ne ha titolarità, dovrà essere esercitata con la firma digitale.

5. Utilizzo della firma digitale

La firma digitale è uno strumento e come tale deve essere utilizzato nei modi e nei casi appropriati. Ricordiamo che non è corretto il suo utilizzo come sistema di identificazione in rete, per il quale esistono strumenti quali la carta d'identità elettronica e le carte di accesso ai servizi.
La firma digitale è utile nel momento in cui è necessario sottoscrivere una dichiarazione ottenendo la garanzia di **integrità** dei dati oggetto della sottoscrizione e di **autenticità** delle informazioni relative al sottoscrittore.
La garanzia che il documento informatico, dopo la sottoscrizione, non possa essere modificato in alcun modo in quanto, durante la procedura di verifica, eventuali modifiche sarebbero riscontrate, la certezza che solo il titolare del certificato possa aver sottoscritto il documento perché non solo possiede il dispositivo di firma (smartcard/tokenUSB) necessario, ma è anche l'unico a conoscere il PIN (Personal Identification Number) necessario per utilizzare il dispositivo stesso, unite al ruolo del certificatore che garantisce la veridicità e la correttezza delle informazioni riportate nel certificato (dati anagrafici del titolare), forniscono allo strumento "firma digitale" caratteristiche tali da non consentire al sottoscrittore di disconoscere la propria firma digitale (fatta salva la possibilità di querela di falso).
Esempi tipici dell'utilizzo della firma digitale possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, dichiarazioni di cambi di residenza, di domicilio, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc.
Fra privati può trovare un interessante impiego nella sottoscrizione di contratti, verbali di riunioni, ordini di acquisto, risposte a bandi di gara, ecc.
Ancora, la firma digitale trova già da tempo applicazione nel protocollo informatico, nella procedura di archiviazione documentale, nel mandato informatico di pagamento, nei servizi camerali, nelle procedure telematiche d'acquisto, ecc.
Alcuni Comuni che partecipano alla sperimentazione della Carta d'Identità Elettronica hanno dotato i propri cittadini di entrambi gli strumenti (CIE o CNS e Firma Digitale) e sviluppato dei servizi in rete tramite i quali i cittadini possono farsi identificare in rete (CIE/CNS), accedere quindi ai propri dati personali nel pieno rispetto delle norme sulla privacy, e sottoscrivere (firma digitale) dichiarazioni, denunce, ricorsi. Ecco quindi che si intravede l'obiettivo finale: dotarsi di un unico strumento con cui sarà possibile farsi riconoscere e sottoscrivere dichiarazioni, fruendo dei vantaggi derivanti dai servizi in rete.

6. La firma digitale e la direttiva europea sulle firme elettroniche

Come già detto sopra, la firma elettronica viene introdotta dalla Direttiva nell'ambito delle definizioni. Tale definizione è stata riportata nella tabella all'inizio delle presenti Linee Guida.
La lettura della definizione ne evidenzia la genericità, quindi essa si presta a interpretazioni differenti e, conseguentemente, risulta per certi versi ambigua e di difficile attuazione concreta. Essa è e rimane un principio giuridico.
Un piccolo passo in avanti lo consente, sempre nella Direttiva, la definizione di firma elettronica avanzata (per la definizione completa si rimanda all'appendice).
In base a tale definizione si comincia a comprendere che ci si deve confrontare con una molteplicità di tipologie di firma. Dal punto di vista pratico è sufficiente considerare:

a) la firma elettronica (generica) può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici;
b) la firma elettronica avanzata, più sofisticata, consente di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione.

Allo stato dell'arte, solo il sistema a chiavi asimmetriche definito per la firma digitale nella legge italiana "pre-Direttiva", soddisfa i requisiti richiesti per la firma elettronica avanzata.
Nessuna delle due firme descritte soddisfano per la Direttiva il requisito di equivalenza con la firma autografa.
E' necessario quindi fare un ulteriore passo in avanti.

6.1 Firme "leggere" e firme "forti"

Anche se è utilizzato correntemente, all'interno della Direttiva non compare mai il concetto di firma "leggera", né quello di firma "forte". Queste definizioni sono state introdotte dagli addetti ai lavori per sopperire alla mancanza di una definizione esplicita di altre tipologie di firma.
Queste tipologie sono introdotte nell'articolo 5 della Direttiva (vedi Appendice per il testo completo dell'articolo). In particolare il primo comma di questo articolo introduce la tipologia di firma più importante dal punto di vista legale perché equivalente alla sottoscrizione autografa. Spesso ci si riferisce ad essa con il termine firma "forte", mentre fra gli addetti ai lavori, specialmente in campo internazionale, la si indica come "firma 5.1".
La firma "forte" è anch'essa nei termini presentati, un principio giuridico, ma vediamo come può essere realizzata praticamente.
Detta firma è una firma elettronica avanzata perché così si deduce dalla definizione. Essa soddisfa specifiche caratteristiche derivanti dal certificatore. Questo è il soggetto che certifica le chiavi mediante le quali la firma è stata generata. Inoltre deve essere apposta con strumenti sicuri come ad esempio un smart card.
Riassumendo, affinché la firma apposta possa essere considerata equivalente ad una autografa:

a) deve essere basata su un sistema a chiavi asimmetriche;
b) deve essere generata con chiavi certificate con le modalità previste nell'allegato I della Direttiva (vedi appendice);

c) deve essere riconducibile a un sistema di chiavi provenienti da un certificatore operante secondo l'allegato II della Direttiva (vedi appendice) e soggetto a vigilanza da parte di un organo definito (il termine "vigilanza" è proprio del recepimento italiano della Direttiva che utilizza "supervisione". Sempre nel recepimento è stato stabilito che la vigilanza è a carico del Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri);
d) deve essere generata utilizzando un dispositivo sicuro che soddisfi i requisiti dell'allegato III della Direttiva (vedi appendice).

Come si vede, a parte piccole differenze organizzative, la precedente normativa italiana "pre-Direttiva" soddisfa quanto appena riassunto.
I certificatori già iscritti nell'elenco pubblico dei certificatori hanno di fatto le caratteristiche per essere considerati "accreditati" secondo quanto previsto dall'articolo 3, comma 2 della Direttiva. Questo fatto, inoltre, è già stato riconosciuto nel decreto di recepimento della Direttiva (art. 11, comma 2 del D.Lgs. 23 gennaio 2002, n. 10).
Il secondo comma dell'articolo 5 della Direttiva (vedi appendice) conferisce dignità giuridica alle altre tipologie di firma. Esse non sono definibili tecnologicamente a priori. Possono essere generate senza vincoli sugli strumenti e sulla modalità operative. E' ovvio che non offrono garanzie di interoperabilità se non in particolari condizioni di utilizzo come in gruppi chiusi di utenti. Infatti, in questo caso, la comunità di utenti condivide gli strumenti di firma e di verifica della stessa. Un giudice, come stabilito nel citato secondo comma dell'articolo 5 della Direttiva, non potrà rifiutare in giudizio queste firme "leggere", ma la loro ammissibilità nascerà dalla libera convinzione e non dall'obbligo di legge previsto per le firme cosiddette "forti".

7. La diffusione della "firma digitale" in Europa

Nell'ambito del F.E.S.A. (Forum of European Supervisor Authority), il cui scopo è far incontrare rappresentanti dei vari organismi di vigilanza nazionali in Europa per l'armonizzazione dei principi e delle tecniche fondamentali che regolano la materia nei rispettivi Stati, si è proceduto alla verifica della diffusione della firma digitale. Da questa analisi, (eseguita nell'ottobre 2002) è emerso che l'Italia era, con 500.000 certificati lo Stato con la maggiore diffusione di certificati, seguita dalla Norvegia con 32.000, e dalla Germania (26.000).
Nel primo trimestre 2004 il numero dei dispositivi rilasciati in Italia per la firma digitale ha superato 1.250.000 unità.
La firma digitale generata in qualunque Stato membro della Comunità deve, sulla base dei trattati comunitari, essere riconosciuta dagli altri Stati. Al fine di rendere agevole tale mutuo riconoscimento è indispensabile che le norme nazionali di recepimento della Direttiva europea 1999/93/CE sulle firme elettroniche nei rispettivi Stati, forniscano un insieme comune di garanzie e certezze. Anche a tale fine diversi organismi fra cui l'EESSI, la Commissione sancita dall'articolo 9 della citata Direttiva europea, l'ETSI, il FESA, stanno lavorando per affinare la Direttiva stessa e realizzare nel contempo degli standard la cui applicazione consenta appunto di raggiungere un adeguato livello di fiducia in tutta la Comunità.
La diffusione della firma digitale in Europa e il suo utilizzo fra gli Stati è una sfida non da poco.
Basti pensare quanto è stato complicato raggiungere l'interoperabilità, perlomeno nel processo di verifica, in Italia, dove si aveva comunque il grande vantaggio derivante dal fatto che tutti i protagonisti (certificatori e titolari) dovevano sottostare alle medesime norme.

8. Il valore legale della firma digitale in Italia

La firma digitale ha trovato l'impianto legislativo necessario per il proprio utilizzo con la pubblicazione, in data 15 aprile 1999, delle regole tecniche costituite dal DPCM 8 febbraio 1999 (oggi sostituito dal DPCM 13 gennaio 2004).
In data 27 gennaio 2000 veniva incluso, nell'elenco pubblico dei certificatori, il primo soggetto autorizzato a rilasciare dispositivi di firma digitale utilizzabili per poter sottoscrivere documenti informatici con la medesima validità giuridica della firma autografa. Un richiamo ben preciso all'articolo 2702 del codice civile ne sanciva, infatti, la validità giuridica, prevedendo appunto che "*La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta*"
Quindi la firma digitale era giuridicamente valida, fatta salva la possibilità per il presunto sottoscrittore di disconoscerne la paternità. In tale evenienza era la controparte, e non il sottoscrittore, a doverne dimostrare la reale paternità.
Diversamente se una firma è "*legalmente considerata come riconosciuta*", ed è il caso ad esempio di una firma autenticata da un pubblico ufficiale, è il sottoscrittore che, per vederne nulli gli effetti, deve intentare una querela di falso.
Con il recepimento della Direttiva europea sulle firme elettroniche 1999/93/CE le cose sono cambiate.
Difatti, già il primo provvedimento legislativo, il DLGS 23 gennaio 2002, n.10, modificando l'articolo 10 (L) " Forma ed efficacia del documento informatico" del DPR 28 dicembre 2000, n.445 – dove era confluito il DPR 10 novembre 1997, n.513 – modificava, rafforzandolo, il valore giuridico di una sottoscrizione effettuata con firma digitale. Detto articolo, al comma 3, prescrive che " *Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto* "
Quindi, alla sottoscrizione con firma digitale "forte" (quella che possiede le seguenti caratteristiche: 1- è una firma elettronica avanzata, 2- è basata su un certificato qualificato, 3- è generata per mezzo di un dispositivo sicuro per la generazione delle firme) viene data la medesima validità giuridica di una firma autografa autenticata da un pubblico ufficiale.
A tutte le altre possibili tipologie di firme elettroniche, cioè quelle cui mancano uno o più delle tre caratteristiche indicate nel periodo precedente, viene esplicitamente conferito valore probatorio.
In un procedimento legale tali firme elettroniche dovranno essere di volta in volta analizzate dal giudice (che si avvarrà certamente di un perito) che deciderà se ammetterle quali prove in giudizio.
Questa previsione, che è stata resa esplicita per recepire senza dubbio alcuno quanto prescritto dalla Direttiva europea, era già presente nel nostro codice civile in quanto, lo stesso, prevede che nessuna prova in giudizio possa essere ricusata a priori.

9. Dove e come dotarsi di firma digitale

Coloro che intendono dotarsi di quanto necessario per poter sottoscrivere con firma digitale documenti informatici possono rivolgersi ad uno dei soggetti autorizzati: i Certificatori.
L'elenco pubblico dei certificatori è disponibile via Internet per la consultazione ([1]), dove sono anche disponibili i link ai siti web degli stessi sui quali sono indicate le modalità operative da seguire. E' bene precisare che vi sono alcuni soggetti che espletano questa attività esclusivamente per gruppi chiusi di utenti. E' il caso del Centro Tecnico che esercita l'attività di certificatore esclusivamente per le PA appartenenti alla Rete Unitaria della Pubblica Amministrazione, piuttosto che l'Esercito Italiano o il Consiglio Nazionale del Notariato, che svolgono detta attività solo per gli appartenenti alle proprie strutture.
Esclusi questi soggetti vi sono, ad oggi, quattordici certificatori accreditati cui rivolgersi.

9.1 Il kit di firma digitale ed i costi

Per poter generare firme digitali è necessario essere dotati di un dispositivo sicuro per la generazione delle firme (costituito da una smartcard o da un token USB), un lettore di smartcard (nel caso in cui non si utilizzi il token USB), un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso (es. per il cambio del PIN che ne consente l'uso).
I costi del kit completo è variabile da certificatore a certificatore; a titolo orientativo è comunque possibile ottenere il kit completo ad un prezzo di circa 100€. Il certificato ha una scadenza, e deve essere quindi rinnovato periodicamente. In genere hanno una validità di uno o due anni, il rinnovo ha un costo orientativo di 10/15 € per anno. E' bene evidenziare che tutti i certificatori prevedono delle condizioni economiche specifiche per forniture di particolare rilievo.

9.2 I Cittadini

I cittadini che intendono utilizzare la firma digitale dovranno recarsi presso l'autorità di registrazione (RA) del certificatore per l'identificazione, la sottoscrizione del contratto di servizio e fornitura, per consegnare eventuale documentazione comprovante il possesso di titoli qualora desideri che detti titoli siano riportati all'interno del certificato.
Le procedure per richiedere il rilascio del certificato (e la fornitura del dispositivo di firma) sono peculiari di ogni certificatore anche se, nella sostanza, prevedono la medesima attività. Dette procedure sono riportate nel manuale operativo ([2]) di ogni certificatore. Nella scelta del certificatore è bene verificare quali servizi aggiuntivi sono forniti dagli stessi (es. certificato di autenticazione e crittografia), la durata del periodo di validità del certificato ed i costi per il rinnovo.

9.3 Le Imprese

Quando un'impresa decide di dotare un numero considerevole dei propri dipendenti del kit di firma digitale, contatta i vari certificatori per scegliere, sulla base del numero dei kit necessari, del costo

[1] L'elenco è disponibile sul sito CNIPA alla pagina http://www.cnipa.gov.it/site/it-IT/Le_Attivit%c3%a0/Elenco_certificatori.

[2] Anch'essi disponibili presso i siti riportati in nota 1 oltre che presso il sito di ogni certificatore. Inoltre i certificatori sono soliti riportare chiaramente sui propri siti web le modalità per richiedere la fomitura del servizio.

complessivo dell'operazione e dei servizi accessori offerti, quello che meglio soddisfa le proprie esigenze. Inoltre, è piuttosto frequente che vi siano accordi al fine di demandare all'impresa stessa l'attività di registrazione e di verifica dell'identità del titolare del certificato. Questa pratica viene spesso utilizzata in quanto comporta diversi benefici a tutti i soggetti coinvolti (dipendente, impresa e certificatore). Il dipendente non deve recarsi fisicamente presso l'autorità di registrazione del certificatore, l'impresa ha un risparmio notevole in termini di ore lavoro spese dai dipendenti per recarsi presso il certificatore oltre al controllo diretto dei certificati emessi per i propri dipendenti con procedure snelle e rapide che consentono di richiedere sospensioni e revoche dei certificati stessi. Il certificatore trae vantaggio dal fatto che non deve impegnare risorse umane per il riconoscimento dei titolari, la verifica dei titoli e di eventuali incarichi o ruoli svolti per l'impresa richiedente.

9.4 Le pubbliche Amministrazioni

Le pubbliche Amministrazioni possono agire come descritto nel paragrafo precedente per le imprese o, in alternativa, possono richiedere di essere accreditate (iscritte quindi nell'elenco pubblico dei certificatori) utilizzando in realtà le infrastrutture tecnologiche di uno dei soggetti già iscritti nell'elenco pubblico dei certificatori. In questo caso, oltre ai vantaggi descritti nel paragrafo precedente, ottengono il vantaggio di risultare, nella fase di verifica di un documento informatico sottoscritto con firma digitale da un proprio dipendente, quali soggetti che emettono e garantiscono le informazioni inerenti il dipendente stesso.

10. LA PROCEDURA DI FIRMA DIGITALE

Generare una firma digitale richiede la disponibilità del kit di firma digitale che, ricordiamo, è composto dal dispositivo sicuro di generazione della firme (smartcard o token USB), eventuale lettore di smartcard, software di firma in grado di utilizzare lo specifico dispositivo di cui si è dotati. Difatti, mentre è vero che è possibile verificare firme digitali generate utilizzando dispositivi eterogenei, non è possibile (salvo essere dotati di software disegnati a tale scopo) utilizzare dispositivi di firma forniti dal certificatore A con il software di firma fornito dal certificatore B.
La procedura di firma è piuttosto banale: dopo aver reso disponibile il dispositivo, inserendo quindi la smartcard nell'apposito lettore o aver inserito il Token USB nella porta specifica, l'applicazione di firma provvederà a richiedere l'inserimento del PIN di protezione, visualizzerà e richiederà di scegliere quale certificato si intende usare e procederà infine alla generazione della firma.
Ricordiamo infatti che un dispositivo sicuro di firma può contenere diversi certificati, e quindi diverse chiavi private, rilasciati per scopi diversi.
Tipico esempio potrebbe essere quello di un soggetto dotato di tre certificati di sottoscrizione: in qualità di cittadino, quale rappresentante legale di una società, quale componente di una commissione. Detto soggetto selezionerà, in fase di sottoscrizione, l'uno o l'altro certificato dipendentemente dalla natura dell'oggetto che si accinge a sottoscrivere.

10.1 Firma digitale di un singolo documento

La firma digitale di un singolo documento è operativamente dipendente dal software di firma di cui si dispone. Tale software può essere fornito da un certificatore, ma sono disponibili anche numerosi prodotti sviluppati da altre aziende.
Indipendentemente dal prodotto però i passi per la sottoscrizione digitale di un singolo documento sono sempre gli stessi. Vediamo quali.
Bisogna ovviamente disporre di un personal computer al quale preventivamente abbiamo collegato il lettore/scrittore di smart card in base alle indicazioni del fornitore.
Dopo aver attivato il software di firma ci verrà richiesto di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore se non lo si è ancora fatto. All'attivazione del processo di firma ci verrà richiesto di inserire il codice PIN della smart card e dopo qualche secondo potremo salvare un file sottoscritto e pronto per essere utilizzato.
In base alla legislazione vigente sull'interoperabilità della firma digitale il file sottoscritto conserva il suo nome originale, al quale viene aggiunta l'estensione ".p7m". Ne risulta che il file mensa.pdf, dopo la sottoscrizione, diverrà mensa.pdf.p7m e come tale sarà fruito da altre applicazioni.

10.2 Firma digitale con procedure automatiche

In numerose situazioni il procedimento di sottoscrizione può coinvolgere un elevato numero di documenti. Non è quindi efficiente in tali procedimenti l'utilizzo della sottoscrizione "documento per documento" quanto meno perché ogni sottoscrizione richiede la digitazione del PIN di sblocco della smart card di firma.
E' perfettamente legale l'utilizzo di procedure automatiche di sottoscrizione, purché ci si attenga a particolari cautele indicate anche dalla legislazione vigente.
In particolare, è necessario che quando il titolare appone la sua firma mediante una procedura automatica utilizzi una coppia di chiavi diversa da tutte le altre in suo possesso. Questo per identificare

immediatamente, in fase di verifica, il fatto che è stata utilizzata una procedura automatica. Per motivi analoghi, ogni dispositivo di firma utilizzato per procedure automatiche deve disporre di coppie di chiavi differenti, una per dispositivo, anche se il titolare è sempre lo stesso.
L'utilizzo di dispositivi di firma particolari denominati HSM (Hardware Security Module) garantisce migliori prestazioni rispetto alle smart card. E' anche possibile utilizzare particolari applicazioni che consentono di digitare il PIN una sola volta a fronte della sottoscrizione di più documenti, garantendo comunque una chiara informativa circa la natura ed il numero dei documenti che verranno automaticamente sottoscritti.

11. LA PROCEDURA DI VERIFICA

La procedura di verifica della firma digitale apposta ad un documento informatico consiste sostanzialmente nel verificare che:

1. il documento non sia stato modificato dopo la firma;
2. il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
3. il certificato del sottoscrittore non sia scaduto;
4. il certificato del sottoscrittore non sia stato sospeso o revocato.

Per eseguire queste verifiche, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software. Detti software sono forniti dai certificatori ai titolari dei certificati; coloro che non sono dotati di un kit di firma digitale possono altresì utilizzare dei software disponibili per uso personale a titolo gratuito: attualmente ne sono stati segnalati quattro, tre da installare sul proprio PC, il quarto disponibile via web. Detti software freeware sono stati resi disponibili dal CNIPA (Verifica_CT – www.cnipa.gov.it/), dalla Comped (DigitalSign – www.comped.it/), da Postecom (FirmaOK – www.poste.it/online/postecert), dalla società Digitaltrust (Sign'ncrypt – www.signncrypt.it) e da TrustItalia (Signo Reader – https://firmadigitale.trustitalia.it/).
Per eseguire la verifica non è necessario disporre di smartcard e lettore, in sintesi non si deve essere necessariamente dotati del kit di firma digitale.
Per eseguire le verifiche di cui ai punti 1, 2 e 3 è sufficiente essere dotati di un personal computer, di un prodotto utile per la verifica, piuttosto che del collegamento ad Internet per la verifica con il prodotto disponibile via web. Per la verifica al punto 4 è necessario avere accesso ad Internet. Difatti, i software di verifica si collegano alla lista di revoca dove il certificatore che ha emesso il certificato qualificato renderà disponibili le informazioni relative alla sospensione o revoca del certificato nel caso in cui si verifichi.
Per la verifica al punto 2 è necessario che sui software installati sul client siano stati caricati i certificati di certificazione dei soggetti iscritti nell'elenco pubblico.
A tale scopo, nel caso in cui i software forniti non abbiano già i certificati delle CA caricati, è necessario scaricare dal sito preposto ([3]) l'elenco pubblico che contiene detti certificati e procedere alla loro installazione.
La procedura descritta è realizzabile in maniera completamente automatica, eventualmente con la necessità di disporre di una connessione a Internet per la verifica della revoca, che deve necessariamente basarsi su informazioni molto aggiornate, e quindi disponibili esclusivamente in rete. E' possibile, inoltre, che vi siano altre verifiche non effettuabili in modalità automatica.
In particolare, un certificato può avere dei limiti di validità dipendenti dalla natura del documento sottoscritto; a titolo di esempio, è possibile che un certificato qualificato garantisca la validità della firma a meno che essa non venga utilizzata per sottoscrivere contratti che coinvolgono transazioni monetarie che eccedono un limite stabilito dal certificatore. La firma di un contratto al di fuori di tali condizioni è considerata non valida, cioè corrisponde alla mancata sottoscrizione. Limiti di questo tipo non sono verificabili in maniera automatica, e richiedono all'utente di porre attenzione ad eventuali note che, comunque, sono sempre incluse nel certificato relativo alla firma che si sta verificando.

[3] L'elenco è disponibile sul sito CNIPA all'indirizzo http://www.cnipa.gov.it/site/it-IT/Le_Attivit%c3%a0/Elenco_certificatori.

11.1 Esempio di verifica

Per rendere evidente che la procedura di verifica è in realtà molto più complessa da descrivere che da eseguire, in questo paragrafo viene riportato un processo di verifica effettuato con il prodotto FirmaOK. Ipotizziamo quindi di aver ricevuto il documento "mensa.pdf.p7m" sottoscritto con firma digitale.

Puntando il documento con il mouse e premendo il tasto destro, si seleziona verifica (figura 1) o, in alternativa, si apre semplicemente il documento con un doppio click.

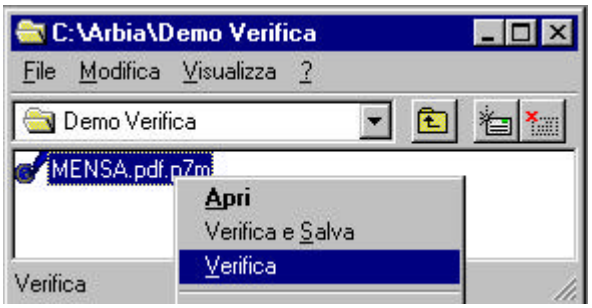

Figura 1

L'applicazione ci presenta subito una finestra dalla quale è possibile evincere che il documento è integro: non è stato quindi modificato dopo essere stato firmato.
Abbiamo quindi assolto la verifica descritta al punto 1 del precedente paragrafo (figura 2).

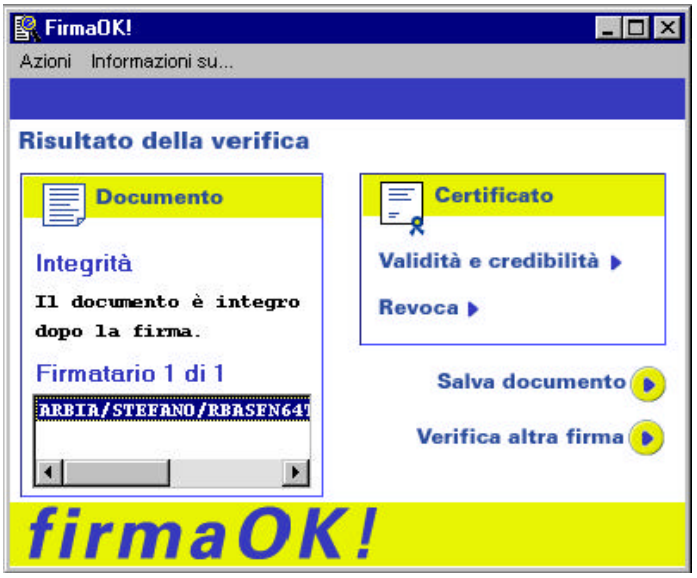

Figura 2

Per verificare che il certificato sia garantito da una CA autorizzata e non sia scaduto (verifiche 2 e 3) selezioniamo "Validità e credibilità".
Viene aperta la finestra mostrata in figura 3 dove si evince che il certificato del Titolare è valido il quanto tale periodo va dal 5 maggio 2003 al 4 maggio 2006, ed è credibile in quanto è stato verificato che lo stesso è sottoscritto, e quindi garantito, da una CA nota.

Figura 3

Selezionando, dalla finestra in figura 2, "Revoca", il prodotto di verifica si collega al certificatore per verificare lo stato del certificato del titolare.
Viene proposta la finestra in figura 4 dove è evidente che alle ore 11:17:01 del 18 luglio 2003, il certificatore ha provveduto ad aggiornare le informazioni di revoca e che il certificato verificato non risulta essere revocato (o sospeso). Verifica al punto 4 eseguita!

Figura 4

A questo punto sappiamo che la sottoscrizione del documento in questione è perfettamente valida, sappiamo chi ha sottoscritto il documento (vedi figura 2), e
possiamo procedere a salvare copia del documento nel formato originale per la visualizzazione.
Selezionando quindi "Salva documento" dalla finestra principale (figura 2) ci viene
chiesto (figura 5) dove salvare il documento a cui viene tolta la firma digitale.

Figura 5

Sarà quindi necessario ricordare che il documento da conservare con le cure del caso è quello inizialmente ricevuto, quello che contiene la firma digitale, riconoscibile dall'estensione "p7m".

Altri prodotti possono ovviamente avere un'interfaccia grafica diversa, modalità operative peculiari, fermo restando che devono possedere funzionalità atte ad eseguire le verifiche descritte precedentemente.

11.2 Procedure automatiche

Nel caso in cui un soggetto realizzi un servizio in rete che prevede l'invio da parte degli utilizzatori di oggetti sottoscritti con firma digitale ovviamente non sarebbe pensabile utilizzare il processo di verifica manuale descritto precedentemente. Sarebbe quindi necessario realizzare una integrazione dell'applicativo destinato alla gestione di suddetto flusso informatico con funzioni di verifica delle rispettive firme digitali. Sono disponibili sul mercato diverse soluzioni che vanno da prodotti specifici le cui funzioni possono essere richiamate da altri applicativi, a librerie e macro specifiche da integrare direttamente nell'applicativo proprietario.

12. Lo strumento "firma digitale" integrato nel processo di e-government

Fino dalla sua nascita la firma digitale è stata una punta di diamante del Governo Italiano nell'ambito dei processi di semplificazione amministrativa. Infatti la firma digitale è indispensabile nell'automazione dei processi amministrativi, nella gestione informatizzata dei flussi documentali e in tutti quei procedimenti dove si vuole l'eliminazione del documento cartaceo (smaterializzazione del procedimento amministrativo).
Sono oramai numerose le applicazioni che utilizzano la firma digitale nell'ambito della pubblica amministrazione. Queste stanno coinvolgendo le imprese, con l'obbligo di trasmissione telematica dei bilanci alle Camere di Commercio, la pubblica amministrazione, con la piena smaterializzazione dei mandati di pagamento con tutti i flussi firmati digitalmente, i cittadini, con la possibilità già descritta precedentemente di inviare istanze e dichiarazioni alla pubblica amministrazione in modalità telematica.
I professionisti saranno sempre più coinvolti nell'utilizzo della firma digitale per gli atti notarili, gli atti giudiziari nell'ambito del processo telematico e per le dichiarazioni fiscali.

La diffusione della Carta d'Identità Elettronica e della Carta Nazionale dei Servizi non potrà che favorire ulteriormente lo sviluppo e il conseguente utilizzo della firma digitale da parte dei cittadini.

A livello internazionale c'è ancora da lavorare per garantire l'interoperabilità almeno a livello comunitario, ma dopo alcuni scetticismi da parte degli organismi comunitari il processo di regolamentazione è avviato anche in tal senso.

Al momento, in ogni caso ci si può dichiarare soddisfatti, visto che l'Italia, primo paese ad avere introdotto la firma digitale nella propria legislazione, è anche il primo paese a superare la soglia del milione di titolari di sottoscrizione digitale (dato ASSOCERTIFICATORI - gennaio 2004).

13. Appendice: la Direttiva Europea 1999/93/CE

L 13/12 IT Gazzetta ufficiale delle Comunità europee 19. 1. 2000

DIRETTIVA 1999/93/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 13 dicembre 1999
relativa ad un quadro comunitario per le firme elettroniche

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare gli articoli 47, paragrafo 2, 55 e 95,

vista la proposta della Commissione (1),

visto il parere del Comitato economico e sociale (2),

visto il parere del Comitato delle regioni (3),

deliberando secondo la procedura di cui all'articolo 251 del trattato (4),

considerando quanto segue:

(1) il 16 aprile 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni una comunicazione relativa ad un'iniziativa europea in materia di commercio elettronico;

(2) l'8 ottobre 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni una comunicazione intitolata «Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche — Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura»;

(3) il 1° dicembre 1997 il Consiglio ha invitato la Commissione a presentare quanto prima una proposta di direttiva del Parlamento europeo e del Consiglio relativa alle firme digitali;

(4) le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati; la divergenza delle norme in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico; invece, un quadro comunitario chiaro relativo alle condizioni che si applicano alle firme elettroniche rafforzerà la fiducia nelle nuove tecnologie e la loro accettazione generale; la normativa negli Stati membri non dovrebbe essere di ostacolo alla libera circolazione di beni e di servizi nel mercato interno;

(5) occorrerebbe promuovere l'interoperabilità dei prodotti di firma elettronica; a norma dell'articolo 14 del trattato, il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci; per garantire la libera circolazione nell'ambito del mercato interno e infondere fiducia nelle firme elettroniche, è necessaria la conformità ai requisiti essenziali specifici relativi ai prodotti di firma elettronica, fatti salvi il regolamento (CE) n. 3381/94 del Consiglio, del 19 dicembre 1994, che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso (5), e la decisione 94/942/PESC del Consiglio del 19 dicembre 1994, relativa all'azione comune adottata dal Consiglio riguardante il controllo delle esportazioni di beni a duplice uso (6);

(6) la presente direttiva non armonizza la fornitura di servizi rispetto al carattere riservato dell'informazione quando sono oggetto di disposizioni nazionali inerenti all'ordine pubblico o alla pubblica sicurezza;

(7) il mercato interno consente anche la libera circolazione delle persone la quale si traduce in una maggiore necessità, per i cittadini dell'Unione europea e per le persone che vi risiedono, di trattare con le autorità di Stati membri diversi da quello in cui risiedono; la disponibilità di comunicazioni elettroniche potrebbe essere di grande aiuto a questo riguardo;

(8) la rapida evoluzione tecnologica e il carattere globale di Internet rendono necessario un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico;

(9) le firme elettroniche verranno usate in svariate circostanze ed applicazioni, che comporteranno un'ampia gamma di nuovi servizi e prodotti facenti uso di firme elettroniche o ad esse collegati; la definizione di tali prodotti e servizi non dovrebbe essere limitata al rilascio e alla gestione di certificati, ma comprenderebbe anche ogni altro servizio e prodotto facente uso di firme elettroniche, o ad esse ausiliario, quali servizi di immatricolazione, servizi di apposizione del giorno e dell'ora, servizi di repertorizzazione, servizi informatici o di consulenza relativi alle firme elettroniche;

(10) il mercato interno consente ai prestatori di servizi di certificazione di sviluppare le proprie attività transfrontaliere al fini di accrescere la competitività e, pertanto, di offrire ai consumatori e alle imprese nuove opportunità di scambiare informazioni e di effettuare negozi per via elettronica in modo sicuro, indipendentemente dalle frontiere; al fine di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte, i prestatori di servizi di certificazione dovrebbero essere liberi di fornire i rispettivi servizi senza preventiva

(1) GU C 325 del 23.10.1998, pag. 5.
(2) GU C 40 del 15.2.1999, pag. 29.
(3) GU C 93 del 6.4.1999, pag. 33.
(4) Parere del Parlamento europeo del 13 gennaio 1999 (GU C 104 del 14.4.1999, pag. 49), posizione comune del Consiglio del 28 giugno 1999 (GU C 243 del 27.8.1999, pag. 33) e decisione del Parlamento europeo del 27 ottobre 1999 (non ancora pubblicata nella Gazzetta ufficiale). Decisione del Consiglio del 30 novembre 1999.

(5) GU L 367 del 31.12.1994, pag. 1. Regolamento modificato dal regolamento (CE) n. 837/95 (GU L 90 del 21.4.1995, pag. 1).
(6) GU L 367 del 31.12.1994, pag. 8. Decisione modificata da ultimo dalla decisione 1999/193/PESC (GU L 73 del 19.3.1999, pag. 1).

autorizzazione; per autorizzazione preventiva non si intende soltanto qualsiasi permesso che il prestatore di servizi interessato deve ottenere dalle autorità nazionali prima di poter fornire i propri servizi di certificazione, ma anche ogni altra misura avente effetto equivalente;

(11) i sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito possono offrire ai prestatori di servizi di certificazione il quadro appropriato per l'ulteriore sviluppo dei loro servizi verso i livelli di fiducia, sicurezza e qualità richiesti dall'evoluzione del mercato; tali sistemi dovrebbero incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; questi ultimi dovrebbero essere liberi di aderire a tali sistemi di accreditamento e di trarne vantaggio;

(12) i servizi di certificazione possono essere forniti o da un'entità pubblica ovvero da una persona giuridica o fisica quando è costituita secondo il diritto nazionale; gli Stati membri non dovrebbero vietare ai prestatori di servizi di certificazione di operare al di fuori dei sistemi di accreditamento facoltativo; si dovrebbe garantire che tali sistemi di accreditamento non riducano la concorrenza nel settore dei servizi di certificazione;

(13) gli Stati membri possono decidere come garantire il controllo del rispetto delle disposizioni contenute nella presente direttiva; quest'ultima non esclude l'istituzione di sistemi di controllo basati sul settore privato; la presente direttiva non obbliga i prestatori di servizi di certificazione a chiedere il controllo in base a un qualsiasi sistema d'accreditamento applicabile;

(14) è importante raggiungere l'equilibrio tra le esigenze dei consumatori e le esigenze delle imprese;

(15) considerando che l'allegato III prevede requisiti relativi a dispositivi per la creazione di una firma sicura al fine di assicurare la funzionalità delle firme elettroniche avanzate; esso non contempla la globalità dell'ambiente del sistema in cui tali dispositivi operano; il funzionamento del mercato interno impone alla Commissione e agli Stati membri un'azione rapida al fine di permettere la designazione degli organismi preposti alla valutazione della conformità dei dispositivi di firma sicura rispetto all'allegato III; per rispondere alle esigenze del mercato, la valutazione della conformità deve essere tempestiva ed efficiente;

(16) la presente direttiva contribuisce all'uso e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità; le firme elettroniche usate esclusivamente all'interno di sistemi basati su accordi volontari di diritto privato fra un numero determinato di partecipanti non esigono una disciplina legislativa comune; nella misura consentita dal diritto nazionale, andrebbe rispettata la libertà delle parti di accordarsi sulle condizioni di accettazione dei dati firmati in modo elettronico; alle firme elettroniche utilizzate in tali sistemi non dovrebbero essere negate l'efficacia giuridica e l'ammissibilità come mezzo probatorio nei procedimenti giudiziari;

(17) la presente direttiva non è diretta ad armonizzare le normative nazionali sui contratti, in particolare in materia di conclusione ed esecuzione dei contratti, od altre formalità di natura extracontrattuale concernenti l'apposizione di firme; per tale motivo, le disposizioni sugli effetti giuridici delle firme elettroniche non dovrebbero pregiudicare i requisiti formali previsti dal diritto nazionale sulla conclusione dei contratti o le regole di determinazione del luogo della conclusione del contratto;

(18) la registrazione e la copia di dati per la creazione di una firma potrebbero costituire una minaccia per la validità giuridica delle firme elettroniche;

(19) le firme elettroniche saranno utilizzate nel settore pubblico nell'ambito delle amministrazioni nazionali e comunitarie e nelle comunicazioni tra tali amministrazioni nonché con i cittadini e gli operatori economici, ad esempio nei settori degli appalti pubblici, della fiscalità, della previdenza sociale, della sanità e dell'amministrazione della giustizia;

(20) criteri armonizzati relativi agli effetti giuridici delle firme elettroniche manterranno un quadro giuridico coerente in tutta la Comunità; il diritto nazionale stabilisce differenti requisiti per la validità giuridica delle firme autografe; i certificati possono essere usati per confermare l'identità di una persona che ricorre alla firma elettronica; le firme elettroniche avanzate basate su un certificato qualificato mirano ad un più alto livello di sicurezza; le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura possono essere considerate giuridicamente equivalenti alle firme autografe solo se sono rispettati i requisiti per le firme autografe;

(21) al fine di contribuire all'accettazione generale dei metodi di autenticazione elettronici, è necessario garantire che le firme elettroniche possano essere utilizzate come prove nei procedimenti giudiziari in tutti gli Stati membri; il riconoscimento giuridico delle firme elettroniche dovrebbe basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione rilasciata al prestatore di servizi di certificazione interessato; il diritto nazionale disciplina la definizione dei campi giuridici in cui possono essere impiegati documenti elettronici e firme elettroniche; la presente direttiva lascia impregiudicata la facoltà degli organi giurisdizionali nazionali di deliberare in merito alla conformità rispetto ai requisiti della presente direttiva e non lede le norme nazionali in materia di libero uso delle prove in giudizio;

(22) la responsabilità dei prestatori di servizi di certificazione che forniscono tali servizi al pubblico è disciplinata dal diritto nazionale;

(23) lo sviluppo del commercio elettronico internazionale rende necessarie soluzioni transfrontaliere che coinvolgano i paesi terzi; al fine di assicurare l'interoperabilità a livello globale, potrebbero essere utili accordi su regole multilaterali con paesi terzi concernenti il riconoscimento reciproco dei servizi di certificazione;

(24) al fine di accrescere la fiducia da parte degli utenti nelle comunicazioni elettroniche e nel commercio elettronico, i prestatori di servizi di certificazione devono osservare la legislazione in materia di protezione dei dati e la vita privata degli individui;

(25) le disposizioni sull'uso degli pseudonimi nei certificati non dovrebbe impedire agli Stati membri di chiedere l'identificazione delle persone in base alla normativa comunitaria o alla legislazione nazionale;

(26) le misure necessarie per l'attuazione della presente direttiva devono essere adottate ai sensi dell'articolo 2 della decisione 1999/468/CE del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione [1];

(27) due anni dopo la sua attuazione la Commissione presenterà una relazione su questa direttiva al fine di garantire tra l'altro che il progresso tecnologico o il mutamento del quadro giuridico non abbiano creato ostacoli al raggiungimento degli obiettivi sanciti nella stessa; la Commissione dovrebbe esaminare le implicazioni dei settori tecnici connessi e presentare una relazione al riguardo al Parlamento europeo e al Consiglio;

(28) secondo i principi di sussidiarietà e proporzionalità di cui all'articolo 5 del trattato, l'obiettivo della creazione di un quadro giuridico armonizzato per la fornitura di firme elettroniche e dei servizi relativi non può essere sufficientemente realizzato dagli Stati membri e può dunque essere realizzato meglio a livello comunitario; la presente direttiva non va al di là di quanto necessario per il raggiungimento degli obiettivi del trattato,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Ambito di applicazione

La presente direttiva è volta ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico. Essa istituisce un quadro giuridico per le firme elettroniche e taluni servizi di certificazione al fine di garantire il corretto funzionamento del mercato interno.

Essa non disciplina aspetti relativi alla conclusione e alla validità dei contratti o altri obblighi giuridici quando esistono requisiti relativi alla forma prescritti dal diritto nazionale o comunitario, né pregiudica le norme e i limiti che disciplinano l'uso dei documenti contenuti nel diritto nazionale o comunitario.

Articolo 2

Definizioni

Ai fini della presente direttiva, valgono le seguenti definizioni:

1) «firma elettronica», dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;

2) «firma elettronica avanzata», una firma elettronica che soddisfi i seguenti requisiti:

   a) essere connessa in maniera unica al firmatario;

   b) essere idonea ad identificare il firmatario;

   c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;

   d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;

3) «firmatario», una persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;

4) «dati per la creazione di una firma», dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;

5) «dispositivo per la creazione di una firma», un software configurato o un hardware usato per applicare i dati per la creazione di una firma;

6) «dispositivo per la creazione di una firma sicura», un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'allegato III;

7) «dati per la verifica della firma», dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;

8) «dispositivo di verifica della firma», un software configurato o un hardware usato per applicare i dati di verifica della firma;

9) «certificato», un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona;

10) «certificato qualificato», un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;

11) «prestatore di servizi di certificazione», un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;

12) «prodotto di firma elettronica», hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche;

13) «accreditamento facoltativo», qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo.

[1] GU L 184 del 17.7.1999, pag. 23.

Articolo 3

Accesso al mercato

1. Gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione.

2. Fatto salvo il paragrafo 1, gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi volti a fornire servizi di certificazione di livello più elevato. Tutte le condizioni relative a tali sistemi devono essere obiettive, trasparenti, proporzionate e non discriminatorie. Gli Stati membri non possono limitare il numero di prestatori di servizi di certificazione accreditati per motivi che rientrano nell'ambito di applicazione della presente direttiva.

3. Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilasci al pubblico certificati qualificati.

4. La conformità dei dispositivi per la creazione di una firma sicura ai requisiti di cui all'allegato III è determinata dai pertinenti organismi pubblici o privati designati dagli Stati membri. Secondo la procedura di cui all'articolo 9 la Commissione fissa i criteri in base ai quali gli Stati membri stabiliscono se un organismo può essere designato.

La conformità ai requisiti di cui all'allegato III accertata dagli organismi di cui al primo comma è riconosciuta da tutti gli Stati membri.

5. Secondo la procedura di cui all'articolo 9 la Commissione può determinare e pubblicare nella *Gazzetta ufficiale delle Comunità europee* i numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica. Un prodotto di firma elettronica conforme a tali norme viene considerato dagli Stati membri conforme ai requisiti di cui all'allegato II, lettera f) e all'allegato III.

6. Gli Stati membri e la Commissione cooperano per promuovere lo sviluppo e l'uso dei dispositivi di verifica della firma, alla luce delle raccomandazioni per la verifica della firma sicura di cui all'allegato IV e nell'interesse dei consumatori.

7. Gli Stati membri possono assoggettare l'uso delle firme elettroniche nel settore pubblico ad eventuali requisiti supplementari. Tali requisiti debbono essere obiettivi, trasparenti, proporzionati e non discriminatori e riguardare unicamente le caratteristiche specifiche dell'uso di cui trattasi. Tali requisiti non possono rappresentare un ostacolo ai servizi transfrontalieri per i cittadini.

Articolo 4

Principi del mercato interno

1. Ciascuno Stato membro applica le disposizioni nazionali da esso adottate in base alla presente direttiva ai prestatori di servizi di certificazione stabiliti nel suo territorio e ai servizi da essi forniti. Gli Stati membri non possono limitare la prestazione di servizi di certificazione originati in un altro Stato membro nella materia disciplinata dalla presente direttiva.

2. Gli Stati membri consentono ai prodotti di firma elettronica conformi alla presente direttiva di circolare liberamente nel mercato interno.

Articolo 5

Effetti giuridici delle firme elettroniche

1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:

a) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e

b) siano ammesse come prova in giudizio.

2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:

— in forma elettronica, o

— non basata su un certificato qualificato, o

— non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero

— non creata da un dispositivo per la creazione di una firma sicura.

Articolo 6

Responsabilità

1. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico tale certificato, sia responsabile per danni provocati a entità o persone fisiche o giuridiche che facciano ragionevole affidamento su detto certificato:

a) per quanto riguarda l'esattezza di tutte le informazioni contenute nel certificato qualificato a partire dalla data di rilascio e il fatto che esso contenga tutti i dati prescritti per un certificato qualificato,

b) per la garanzia che, al momento del rilascio del certificato, il firmatario identificato nel certificato qualificato detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato,

c) la garanzia che i dati per la creazione della firma e i dati per la verifica della firma possano essere usati in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi entrambi,

a meno che il prestatore di servizi di certificazione provi di aver agito senza negligenza.

2. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato sia responsabile, nei confronti di entità o di persone fisiche o giuridiche che facciano ragionevole affidamento sul certificato, dei danni provocati, per la mancata registrazione della revoca del certificato, a meno che provi di aver agito senza negligenza.

3. Gli Stati membri provvedono a che un prestatore di servizi di certificazione possa indicare, in un certificato qualificato, i limiti d'uso di detto certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione deve essere esentato dalla responsabilità per i danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti nello stesso.

4. Gli Stati membri provvedono affinché un prestatore di servizi di certificazione abbia la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato, purché tali limiti siano riconoscibili da parte dei terzi.

Il prestatore di servizi di certificazione non è responsabile dei danni risultanti dal superamento di detto limite massimo.

5. I paragrafi da 1 a 4 lasciano impregiudicata la direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (4).

Articolo 7

Aspetti internazionali

1. Gli Stati membri provvedono a che i certificati rilasciati al pubblico come certificati qualificati da un prestatore di servizi di certificazione stabilito in un paese terzo siano riconosciuti giuridicamente equivalenti ai certificati rilasciati da un prestatore di servizi di certificazione stabilito nella Comunità, in presenza di una delle seguenti condizioni:

a) il prestatore di servizi di certificazione possiede i requisiti di cui alla presente direttiva e sia stato accreditato in virtù di un sistema di accreditamento facoltativo stabilito in uno Stato membro, oppure

b) il certificato è garantito da un prestatore di servizi di certificazione stabilito nella Comunità, in possesso dei requisiti di cui alla presente direttiva, oppure

c) il certificato o il prestatore di servizi di certificazione è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e paesi terzi o organizzazioni internazionali.

2. Al fine di agevolare servizi di certificazione transfrontalieri con paesi terzi e il riconoscimento giuridico delle firme elettroniche avanzate che hanno origine in paesi terzi, la Commissione presenta, se del caso, proposte miranti all'effettiva attuazione di norme e di accordi internazionali applicabili ai servizi di certificazione. In particolare, ove necessario, essa presenta al Consiglio proposte relative a mandati per la negoziazione di accordi bilaterali e multilaterali con paesi terzi e organizzazioni internazionali. Il Consiglio decide a maggioranza qualificata.

3. Ogniqualvolta la Commissione è informata di difficoltà che le imprese comunitarie incontrano riguardo all'accesso al mercato di paesi terzi, essa può, se necessario, presentare al Consiglio proposte in merito a un appropriato mandato di negoziato per ottenere diritti paragonabili per le imprese comunitarie in tali paesi terzi. Il Consiglio decide a maggioranza qualificata.

Le misure adottate a norma di questo paragrafo lasciano impregiudicati gli obblighi della Comunità e degli Stati membri derivanti da accordi internazionali in materia.

Articolo 8

Protezione dei dati

1. Gli Stati membri provvedono a che i prestatori di servizi di certificazione e gli organismi nazionali responsabili dell'accreditamento o della supervisione si conformino alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (5).

2. Gli Stati membri consentono a un prestatore di servizi di certificazione che rilascia certificati al pubblico di raccogliere dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

3. Fatti salvi gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi, gli Stati membri non vietano al prestatore di servizi di certificazione di riportare sul certificato uno pseudonimo in luogo del nome del firmatario.

Articolo 9

Comitato

1. La Commissione è assistita da un «comitato per la firma elettronica», in prosieguo denominato «il comitato».

2. Nei casi in cui si fa riferimento al presente paragrafo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE, tenuto conto dell'articolo 8 della stessa.

Il periodo di cui all'articolo 4, paragrafo 3 della decisione 1999/468/CE è fissato a tre mesi.

3. Il comitato adotta il proprio regolamento interno.

Articolo 10

Compiti del comitato

Il comitato precisa i requisiti di cui agli allegati della presente direttiva, i criteri di cui all'articolo 3, paragrafo 4 e le norme generalmente riconosciute per i prodotti di firma elettronica istituite e pubblicate a norma dell'articolo 3, paragrafo 5, secondo la procedura di cui all'articolo 9, paragrafo 2.

(4) GU L 95 del 21.4.1993, pag. 29.

(5) GU L 281 del 23.11.1995, pag. 31.

Articolo 11

Notificazione

1. Gli Stati membri comunicano alla Commissione e agli altri Stati membri le seguenti informazioni:

a) sistemi di accreditamento facoltativi nazionali ed ogni requisito supplementare a norma dell'articolo 3, paragrafo 7;

b) nomi e indirizzi degli organismi nazionali responsabili dell'accreditamento e della supervisione nonché degli organismi di cui all'articolo 3, paragrafo 4;

c) i nomi e gli indirizzi di tutti i prestatori di servizi di certificazione nazionali accreditati.

2. Le informazioni di cui al paragrafo 1 e le loro eventuali variazioni sono notificate agli Stati membri al più presto.

Articolo 12

Riesame

1. Entro il 19 luglio 2003 la Commissione riesamina l'applicazione della presente direttiva e presenta una relazione in merito al Parlamento europeo e al Consiglio.

2. Nel riesame si valuta, tra l'altro, se l'ambito di applicazione della presente direttiva debba essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. La relazione include in particolare una valutazione, sulla base dell'esperienza acquisita, degli aspetti relativi all'armonizzazione. La relazione è corredata, se del caso, di proposte legislative.

Articolo 13

Attuazione

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva anteriormente al 19 luglio 2001. Essi ne informano immediatamente la Commissione.

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle principali disposizioni di diritto interno che adottano nella materia disciplinata dalla presente direttiva.

Articolo 14

Entrata in vigore

La presente direttiva entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

Articolo 15

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, addì 13 dicembre 1999.

Per il Parlamento europeo	*Per il Consiglio*
La Presidente	*Il Presidente*
N. FONTAINE	S. HASSI

ALLEGATO I

Requisiti relativi ai certificati qualificati

I certificati qualificati devono includere:

a) l'indicazione che il certificato rilasciato è un certificato qualificato;

b) l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;

c) il nome del firmatario del certificato o uno pseudonimo identificato come tale;

d) l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;

e) i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;

f) un'indicazione dell'inizio e del termine del periodo di validità del certificato;

g) il codice d'identificazione del certificato;

h) la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;

i) i limiti d'uso del certificato, ove applicabili; e

j) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

ALLEGATO II

Requisiti relativi ai prestatori di servizi di certificazione che rilasciano certificati qualificati

I prestatori di servizi di certificazione devono:

a) dimostrare l'affidabilità necessaria per fornire servizi di certificazione;

b) assicurare il funzionamento di un servizio di repertoriazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;

c) assicurare che la data e l'ora di rilascio o di revoca di un certificato possano essere determinate con precisione;

d) verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato;

e) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute;

f) utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;

g) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza nel corso della generazione di tali dati;

h) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione;

i) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;

j) non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave;

k) prima di avviare una relazione contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

l) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:

— soltanto le persone autorizzate possano effettuare inserimenti e modifiche;

— l'autenticità delle informazioni sia verificabile;

— i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato;

— l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

ALLEGATO III

Requisiti relativi ai dispositivi per la creazione di una firma sicura

1. I dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che:

   a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è ragionevolmente garantita la loro riservatezza;

   b) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro limiti ragionevoli di sicurezza, essere derivati e la firma è protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile;

   c) i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi per la creazione di una firma sicura non devono alterare i dati da firmare né impediscono che tali dati siano presentati al firmatario prima dell'operazione di firma.

ALLEGATO IV

Raccomandazioni per la verifica della firma sicura

Durante il processo relativo alla verifica della firma occorre garantire, entro limiti ragionevoli di certezza, che:

a) i dati utilizzati per la verifica della firma corrispondono ai dati comunicati al verificatore;

b) la firma è verificata in modo affidabile e i risultati della verifica correttamente comunicati;

c) il verificatore può, all'occorrenza, stabilire in modo attendibile i contenuti dei dati firmati;

d) l'autenticità e la validità del certificato necessario al momento della verifica della firma sono verificate in modo attendibile;

e) i risultati della verifica e dell'identità del firmatario sono comunicati correttamente;

f) l'uso di uno pseudonimo è chiaramente indicato;

g) qualsiasi modifica che incida sulla sicurezza può essere individuata.