CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

La normativa sulla firma elettronica

Segreteria tecnica e Comunicazione
Sezione Pubblicazioni e sito web
comunicazione@cnipa.it
tel. 06 85264.207

via Isonzo, 21/b – 00198 Roma

www.cnipa.gov.it

14

COLLANA MINIGRAFIE CNIPA:

- n. 1 La Televisione Digitale Terrestre
- n. 2 La Legge Stanca e il suo regolamento di attuazione
- n. 3 La Legge Stanca: i requisiti di accessibilità
- n. 4 Scuola virtuale della Pubblica Amministrazione
- n. 5 Il Portale Nazionale delle Imprese
- n. 6 Dal CNIPA un servizio reale: il "protocollo in ASP" per la PA
- n. 7 La Normativa italiana sull'Accessibilità
- n. 8 La qualità dei beni e servizi nei contratti della Pubblica Amministrazione: linee guida per una migliore gestione
- n. 9 Cos'è il Cnipa
- n. 10 La Continuità Operativa delle pubbliche amministrazioni
- n. 11 La posta elettronica certificata
- n. 12 L'iniziativa "Lotta agli sprechi"
- n. 13 Codice dell'amministrazione digitale

CNIPA - Centro Nazionale per l'Informatica nella Pubblica Amministrazione
via Isonzo, 21b - 00198 Roma
tel. 06 85264.1 – www.cnipa.gov.it

Finito di stampare nel mese di ottobre 2006 dagli Stabilimenti Tipografici Carlo Colombo S.p.A.
Via Roberto Malatesta, 296 - 00176 Roma

La normativa sulla firma elettronica

Pubblicazione a cura di Giovanni Manca

Coordinamento redazionale
Barbara Pasculli
Alessandro Staiti

Sommario

Introduzione

La storia italiana del documento informatico e della firma digitale inizia con l'articolo 15, comma 2 della Legge 15 marzo 1997, n. 59.
"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge."
La stessa legge conferisce delega per l'emanazione di specifici regolamenti che definiscono i criteri di applicazione. Tale delega viene attuata con il D.P.R. 10 novembre 1997, n. 513 (G.U. 13 marzo 1998, n. 60). Seguono a breve le regole tecniche sulla materia con il D.P.C.M. 8 febbraio 1999 (G.U. 15 aprile 1999, n. 87).
Il sistema legislativo italiano è così completo e parte rapidamente riconoscendo, nell'arco di pochi mesi, il ruolo di certificatore per la firma digitale a ben otto soggetti.
All'inizio del 2000 viene pubblicata nella Gazzetta Ufficiale comunitaria la direttiva 1999/93/CE relativa a un quadro comunitario per le firme elettroniche (G.U.C.E. n. L 013, 19 gennaio 2000). Tale direttiva arriva praticamente in contemporanea con il riordinamento del documento amministrativo operato mediante il D.P.R. 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (G.U. 20 febbraio 2001, n. 42 suppl. ord.).
Le regole europee aprono un esteso dibattito su come procedere al loro recepimento. L'Europa ha obiettivi diversi da quelli delle norme italiane del 1997. Queste hanno come obiettivo centrale l'attribuzione di specifici effetti giuridici ai documenti informatici al fine di, come si dice spesso, eliminare la carta nel procedimento amministrativo. I benefici riguardano la pubblica amministrazione e i privati.
Il testo europeo vede invece al centro il mercato: il commercio elettronico ha bisogno di regole comuni per garantire la libera circolazione dei prodotti dell'industria. Viene introdotta una definizione di sottoscrizione autografa estremamente complessa, "firma elettronica avanzata, basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma". La normativa europea definisce anche la firma elettronica, sostanzialmente un metodo informatico di autenticazione che nel linguaggio cor-

rente viene identificata anche come “firma leggera”. La sottoscrizione digitale equivalente a quella autografa diviene “firma forte”.
Il recepimento delle disposizioni europee avviene con il D.lgs. 23 gennaio 2002, n. 10 (G.U. 15 febbraio 2002, n. 39), poi assorbito, con modifiche, dal Codice dell’amministrazione digitale [D.lgs. 7 marzo 2005, n. 82 (il Codice è stato integrato con il D.lgs. 4 aprile 2006, n. 159)].
L’evoluzione tecnologica rende necessario l’aggiornamento delle regole tecniche che vengono stabilite con il D.P.C.M. 13 gennaio 2004 (G.U. 27 aprile 2004, n. 98).
Tali regole tecniche sono ancora valide anche se l’entrata in vigore del Codice dell’amministrazione digitale richiede che esse siano aggiornate per il coordinamento dei testi.
Il Codice dell’amministrazione digitale stabilisce le nuove regole per il documento informatico e la firma elettronica. Quest’ultima si consolida nell’ordinamento nelle forme di firma elettronica c.d. “leggera” e di firma elettronica qualificata, categoria nella quale rientra la firma digitale, la cui apposizione al documento informatico definisce giuridicamente quest’ultimo come pienamente equivalente dal punto di vista giuridico al documento cartaceo con sottoscrizione autografa, cioè alla scrittura privata.
La firma digitale rappresenta quindi la realizzazione pratica della firma elettronica qualificata utilizzando una coppia di chiavi crittografiche asimmetriche. Il percorso attuale si ricongiunge con quello iniziato nel D.P.R. 513 del 1997 ed anche la direttiva europea trova una sua piena realizzazione nelle nuove regole legislative.
La firma digitale diventa così lo strumento abilitante per l’intero sistema della dematerializzazione del documento. Essa può essere pienamente utilizzata non solo per la sottoscrizione del documento informatico, ma anche nella conservazione documentale sostitutiva, nella fatturazione elettronica, nello scambio di documenti informatici in procedimenti amministrativi che hanno eliminato la carta, come strumento di autenticazione in rete nei confronti della P.A.. Ma la tecnologia non sta ferma e nuove regole devono essere emanate per tenere il passo.
In attesa delle modifiche al D.P.C.M. 13 gennaio 2004, necessarie per il coordinamento con il Codice dell’amministrazione digitale, altre regole tecniche sono state emanate per garantire l’interoperabilità, fondamentale elemento per l’efficace riconoscimento e verifica del documento informatico. Il sistema italiano, di riferimento a livello mondiale, ha sviluppato delle regole di interoperabilità complete e aggiornate allo stato dell’arte degli standard internazionali.

Infine le esigenze innovative dei flussi documentali hanno richiesto ulteriori, specifiche regole per i nuovi e diffusissimi formati documentali PDF (Portable Document Format) e XML (eXchange Markup Language). Tali regole sono state stabilite nelle Deliberazioni CNIPA n. 4 del 17 febbraio 2005 (G.U. del 3 marzo 2005, n. 51) e n. 34 del 18 maggio 2006 (G.U. del 3 ottobre 2006, n. 230).
Come si vede il primo decennio della firma digitale è stato ricco di episodi, di ostacoli superati e risultati positivi.

NORME EUROPEE

Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche[1]

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[2],

visto il parere del Comitato economico e sociale[3],

visto il parere del Comitato delle regioni[4],

deliberando secondo la procedura di cui all'articolo 251 del trattato[5],

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

[1] Incluse le rettifiche introdotte dalla Gazzetta Ufficiale delle Comunità europee L 119/4 del 7 maggio 2002.
[2] GU C 325 del 23.10.1998, pag. 5.
[3] GU C 40 del 15.2.1999, pag. 29.
[4] GU C 93 del 6.4.1999, pag. 33.
[5] 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.

l'affidabilità nelle comunicazioni elettroniche – Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura";

(3) il 10 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[6], 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[7];

(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

[6] 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).

[7] 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).

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 ai 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 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 dovrebbero 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[8];

(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 giuri-

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

dico 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"[9], un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'allegato III;

[9] La dizione "dispositivo di firma sicura" deriva da un'errata traduzione dall'inglese: la versione corretta è "dispositivo sicuro di firma". Questo errore ricorre più volte nel testo della Direttiva.

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.

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 al momento del 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 en-

trambi, 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[10].

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

[10] GU L 95 del 21.4.1993, pag. 29.

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[11].

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

[11] GU L 281 del 23.11.1995, pag. 31.

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.

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.

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 repertorizzazione 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 sicuri per la creazione di una firma 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.

Decisione della Commissione del 6 novembre 2000 relativa ai criteri minimi di cui devono tener conto gli Stati membri all'atto di designare gli organismi di cui all'articolo 3, paragrafo 4, della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche[12] e in particolare l'articolo 3, paragrafo 4, considerando quanto segue:

(1) Il 13 dicembre 1999 il Parlamento europeo e il Consiglio hanno adottato la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

[12] GU L 13 del 19.1.2000, pag. 12.

(2) L'allegato III della direttiva 1999/93/CE stabilisce i requisiti relativi ai dispositivi per la creazione di una firma sicura. Conformemente all'articolo 3, paragrafo 4, della direttiva, 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, mentre la Commissione fissa i criteri in base ai quali gli Stati membri stabiliscono se un organismo può essere designato per determinare tale conformità.

(3) La Commissione fissa i summenzionati criteri previa consultazione del comitato per la firma elettronica istituito a norma dell'articolo 9, paragrafo 1, della direttiva 1999/93/CE.

(4) Le misure previste dalla presente direttiva sono conformi al parere del comitato per la firma elettronica,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La presente direttiva stabilisce i criteri in base ai quali gli Stati membri designano gli organismi incaricati di determinare la conformità dei dispositivi per la creazione di una firma sicura.

Articolo 2

Qualora appartenga ad un'organizzazione che svolge attività diverse dalla valutazione della conformità dei dispositivi per la creazione di una firma sicura ai requisiti stabiliti nell'allegato III della direttiva 1999/93/CE, l'organismo designato è chiaramente identificabile all'interno di detta organizzazione. Le diverse attività sono chiaramente distinte.

Articolo 3

L'organismo e il suo personale non intraprendono attività che rischino di interferire con la loro indipendenza di giudizio e la loro integrità in relazione ai compiti loro affidati. In particolare, l'organismo è indipendente dalle parti in presenza. Di conseguenza, l'organismo, il suo direttore esecutivo e il personale incaricato della verifica di conformità non devono essere progettisti, fabbricanti, fornitori o installatori di dispositivi per la creazione di una firma sicura, né fornitori di servizi di certificazione che rilasciano certi-

ficati al pubblico, né rappresentanti autorizzati delle suddette parti. Gli organismi godono di indipendenza finanziaria e non partecipano direttamente ad attività di progettazione, costruzione, commercializzazione o manutenzione di dispositivi per la creazione di una firma sicura, né rappresentano parti coinvolte in tali attività. Quanto precede non osta alla possibilità di scambio di informazioni tecniche tra il fabbricante e l'organismo notificato.

Articolo 4

L'organismo e il suo personale sono in grado di determinare la conformità dei dispositivi per la creazione di una firma sicura ai requisiti stabiliti dall'allegato III della direttiva 1999/93/CE dando prova di alta integrità professionale, affidabilità e sufficiente competenza tecnica.

Articolo 5

L'organismo applica procedure di valutazione della conformità trasparenti e registra tutte le informazioni pertinenti riguardanti tali attività. Tutte le parti interessate hanno accesso ai servizi dell'organismo. Il funzionamento dell'organismo risponde a procedure gestite in modo non discriminatorio.

Articolo 6

L'organismo dispone delle risorse umane e materiali sufficienti per svolgere correttamente e speditamente i compiti tecnici ed amministrativi connessi con le attività per le quali è stato designato.

Articolo 7

Il personale responsabile della valutazione di conformità possiede:

- una solida formazione tecnica e professionale, in particolare nel campo delle tecnologie di firma elettronica e dei corrispondenti aspetti di sicurezza delle tecnologie dell'informazione,
- una buona conoscenza delle esigenze legate alle valutazioni di conformità che realizza nonché l'esperienza necessaria per realizzare tali valutazioni.

Articolo 8

È garantita l'imparzialità del personale. La sua retribuzione non dipende dal numero di valutazioni di conformità effettuate né dal loro risultato.

Articolo 9

L'organismo prende le necessarie disposizioni per la copertura delle responsabilità derivanti dalle proprie attività mediante, ad esempio, un'adeguata assicurazione.

Articolo 10

L'organismo prende le necessarie disposizioni per garantire la riservatezza delle informazioni ottenute nell'esecuzione delle attività previste dalla direttiva 1999/93/CE o da qualsiasi disposizione nazionale di applicazione della stessa, salvo nei confronti delle competenti autorità dello Stato membro che lo ha designato.

Articolo 11

Qualora un organismo designato prenda disposizioni perché parte della valutazione di conformità sia realizzata da una terza parte, garantisce ed è in grado di dimostrare che quest'ultima dispone della competenza necessaria per realizzare il servizio in questione. L'organismo designato assume l'intera responsabilità delle attività realizzate nell'ambito di tali disposizioni. La decisione finale spetta all'organismo designato.

Articolo 12

Gli Stati membri sono destinatari della presente decisione.

Decisione della Commissione del 14 luglio 2003 relativa alla pubblicazione dei numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroni-

che[13], in particolare l'articolo 3, paragrafo 5, considerando quanto segue:

(1) L'allegato II, lettera f) e l'allegato III della direttiva 1999/ 93/CE fissano i requisiti dei prodotti di firma elettronica sicuri.

(2) Le specifiche tecniche necessarie per la produzione e la commercializzazione di prodotti basati sullo stato dell'arte tecnologico sono elaborate da organismi competenti in materia di normalizzazione.

(3) Il CEN (Comitato europeo di normalizzazione) e l'ETSI (Istituto europeo per le norme di telecomunicazioni) offrono, nell'ambito dell'EESSI (*European Electronic Signature Standardisation initiative*), una piattaforma europea aperta, partecipativa e flessibile per la ricerca di una posizione di consenso attorno allo sviluppo della Società dell'informazione in Europa. Tali organismi hanno sviluppato norme relative a prodotti di firma elettronica (*CWA-CEN workshop agreement* o *ETSI TS-ETSI technical specification*) fondate sui requisiti stabiliti dagli allegati della direttiva 1999/93/CE.

(4) Le misure stabilite nella presente decisione sono conformi al parere del comitato per la firma elettronica,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

I numeri di riferimento delle norme generalmente riconosciute relative a prodotti di firma elettronica figurano nell'allegato.

Articolo 2

La Commissione procede ad un riesame del funzionamento della presente decisione entro due anni dalla data della sua pubblicazione nella Gazzetta ufficiale dell'Unione europea e riferisce al riguardo al comitato istituito ai sensi dell'articolo 9 paragrafo 1 della direttiva 1999/93/CE.

Articolo 3

Gli Stati membri sono destinatari della presente decisione.

[13] GU L 13 del 19.1.2000, pag. 12.

ALLEGATO

A. Elenco delle norme generalmente riconosciute relative ai prodotti di firma elettronica che vengono considerati dagli Stati membri conformi ai requisiti di cui all'allegato II, lettera f) della direttiva 1999/93/CE

- CWA 14167-1 (marzo 2003): *security requirements for trustworthy systems managing certificates for electronic signatures* — Part 1: *System Security Requirements*
- CWA 14167-2 (marzo 2002): *security requirements for trustworthy systems managing certificates for electronic signatures* — Part 2: *cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)*

B. Elenco delle norme generalmente riconosciute relative ai prodotti di firma elettronica che vengono considerati dagli Stati membri conformi ai requisiti di cui all'allegato III della direttiva 1999/93/CE

- CWA 14169 (marzo 2002): *secure signature-creation devices*

NORME ITALIANE

Estratto dal Decreto legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale[14]

Capo I
PRINCIPI GENERALI

Sezione I
Definizioni, finalità e ambito di applicazione

Articolo 1
(Definizioni)

1. Ai fini del presente codice si intende per:

b) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

[14] Testo coordinato con il decreto legislativo 4 aprile 2006, n. 159 recante "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale".

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

r) firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, 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, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, 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;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Capo II
DOCUMENTO INFORMATICO E FIRME ELETTRONICHE; PAGAMENTI, LIBRI E SCRITTURE

Sezione I
Documento informatico

Articolo 20
(Documento informatico)

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Articolo 21

(Valore probatorio del documento informatico sottoscritto)

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

Articolo 22

(Documenti informatici originali e copie. Formazione e conservazione)

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni costituiscono informazione primaria ed ori-

ginale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate, sia il soggetto che ha effettuato l'operazione.

3. Le copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite ai sensi dell'articolo 71, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentito il Garante per la protezione dei dati personali.

Articolo 23

(Copie di atti e documenti informatici)

1. All'articolo 2712 del codice civile dopo le parole:

«riproduzioni fotografiche» è inserita la seguente:

«, informatiche»[15].

2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche.

2-bis. Le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono

[15] Pertanto l'articolo 2712 del codice civile "Riproduzioni meccaniche" diventerà: "Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fotografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime".

ad ogni effetto di legge l'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

4. Le copie su supporto informatico di documenti originali non unici formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è assicurata dal responsabile della conservazione mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.

5. Le copie su supporto informatico di documenti, originali unici, formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Sezione II
Firme elettroniche e certificatori

Articolo 24
(Firma digitale)

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Articolo 25
(Firma autenticata)

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.

4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

Articolo 26
(Certificatori)

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onora-

bilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.

2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.

3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

Articolo 27

(Certificatori qualificati)

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.

2. I certificatori di cui al comma 1, devono inoltre:

a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

4. Il CNIPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

Articolo 28

(Certificati qualificati)

1. I certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;

b) numero di serie o altro codice identificativo del certificato;

c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;

d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;

f) indicazione del termine iniziale e finale del periodo di validità del certificato;

g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice

identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.

3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3.

c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.

Articolo 29

(Accreditamento)

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.

2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.

3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:

a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;

b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.

4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.

8. Sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.

Articolo 30

(Responsabilità del certificatore)

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;

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

c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;

d) sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.

3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Articolo 31

(Vigilanza sull'attività di certificazione)

1. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e accreditati.

Articolo 32

(Obblighi del titolare e del certificatore)

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:

a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;

b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle regole tecniche di cui all'articolo 71;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

f) non rendersi depositario di dati per la creazione della firma del titolare;

g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli 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 in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

5. Il certificatore raccoglie i 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, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Articolo 33

(Uso di pseudonimi)

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.

Articolo 34

(Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati)

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;
b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.

3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.

4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.

5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

Articolo 35

(Dispositivi sicuri e procedure per la generazione della firma)

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

a) sia riservata;

b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;

c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. L'apposizione di firme con procedura automatica è valida se l'attivazione della procedura medesima è chiaramente riconducibile alla volontà del titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente.

4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui al comma 5.

5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Lo schema nazionale la cui attuazione non deve determinare nuovi o maggiori oneri per il bilancio dello Stato ed individua l'organismo pubblico incaricato di accreditare i centri di valutazione e di certificare le valutazioni di sicurezza. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

6. La conformità ai requisiti di sicurezza dei dispositivi sicuri per la creazione di una firma qualificata a quanto prescritto dall'allegato III della direttiva 1999/93/CE è inoltre riconosciuta se certificata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva stessa.

Articolo 36

(Revoca e sospensione dei certificati qualificati)

1. Il certificato qualificato deve essere a cura del certificatore:

a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;

b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;

d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.

3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 71.

Articolo 37

(Cessazione dell'attività)

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al CNIPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.

2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento

della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.

3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.

4. Il CNIPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004

Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici[16]

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e in particolare l'art. 8, comma 2;

visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche;

visto l'art. 15, comma 2, della legge 15 marzo 1997, n. 59;

vista la decisione della Commissione europea 14 luglio 2003, relativa alla pubblicazione dei numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata nella Gazzetta Ufficiale dell'Unione europea L 175/45 del 15 luglio 2003 che induce ad integrare in tal senso le premesse del provvedimento;

visto il decreto del Presidente del Consiglio dei Ministri 9 agosto 2001, con il quale è stata attribuita al Ministro per l'innovazione e le tecnologie, dott. Lucio Stanca, tra l'altro, la delega ad esercitare le funzioni spettanti al Presidente del Consiglio dei Ministri nelle materie dell'innovazione

[16] G.U. 27 aprile 2004, n. 98.

tecnologica, dello sviluppo della società dell'informazione, nonché delle connesse innovazioni per le amministrazioni pubbliche;

sentito il Ministro per la funzione pubblica;

sentito il Garante per la protezione dei dati personali;

espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del 22 giugno 1998, del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE del 20 luglio 1998, CE del Parlamento europeo e del Consiglio, attuata con decreto legislativo 23 novembre 2000, n. 427;

DECRETA:

TITOLO I
Disposizioni generali

1. Definizioni

1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute negli articoli 1 e 22 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni. Si intende, inoltre, per:

a. TESTO UNICO, il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, emanato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b. DIPARTIMENTO, il dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri o altro organismo di cui si avvale il Ministro per l'innovazione e le tecnologie;

c. CHIAVI, la coppia di chiavi asimmetriche come definite all'art. 22, comma 1, lettera b), del testo unico;

d. IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (BIT), la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;

e. FUNZIONE DI HASH, una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali;

f. EVIDENZA INFORMATICA, una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;

g. RIFERIMENTO TEMPORALE, informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;

h. VALIDAZIONE TEMPORALE, il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi;

i. MARCA TEMPORALE, un'evidenza informatica che consente la validazione temporale.

2. Ambito di applicazione

1. Il presente decreto stabilisce, ai sensi dell'art. 8, comma 2, del testo unico, le regole tecniche per la generazione, apposizione e verifica delle firme digitali.

2. Le disposizioni di cui al titolo II si applicano ai certificatori che rilasciano al pubblico certificati qualificati ai sensi del testo unico.

3. Ai certificatori accreditati o che intendono accreditarsi ai sensi del testo unico si applicano, oltre a quanto previsto dal comma 2, anche le disposizioni di cui al titolo III.

4. I certificatori accreditati devono disporre di un sistema di validazione temporale conforme alle disposizioni di cui al titolo IV.

5. Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione europea e dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE, è consentito di circolare liberamente nel mercato interno.

6. Le disposizioni di cui al comma 5 si applicano anche agli Stati non appartenenti all'Unione europea con i quali siano stati stipulati specifici accordi di riconoscimento reciproco.

TITOLO II
REGOLE TECNICHE DI BASE

3. Norme tecniche di riferimento

1. I prodotti di firma digitale e i dispositivi sicuri di firma di cui all'art. 29-sexies del testo unico, devono essere conformi alle norme generalmente

riconosciute a livello internazionale o individuate dalla Commissione europea secondo la procedura di cui all'art. 9 della direttiva 1999/93/CE.

2. Gli algoritmi di generazione e verifica delle firme digitali e le funzioni di hash sono individuati ai sensi del comma 1.

3. Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma, non produce gli effetti di cui all'art. 10, comma 3, del testo unico, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

4. Caratteristiche generali delle chiavi per la creazione e la verifica della firma

1. Una coppia di chiavi per la creazione e la verifica della firma può essere attribuita ad un solo titolare.

2. Se il titolare appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.

3. Se la procedura automatica fa uso di più dispositivi per apporre la firma del medesimo titolare, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo.

4. Ai fini del presente decreto, le chiavi di creazione e verifica della firma ed i correlati servizi, si distinguono secondo le seguenti tipologie:

a. chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b. chiavi di certificazione, destinate alla generazione e verifica delle firme apposte o associate ai certificati qualificati, alle liste di revoca (CRL) e sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c. chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

5. Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, dal precedente comma 4.

6. In deroga a quanto stabilito al comma 5, le chiavi di certificazione di cui al comma 4, lettera b), possono essere utilizzate per altre finalità previa autorizzazione da parte del Dipartimento.

7. La robustezza delle chiavi deve essere tale da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche.

5. Generazione delle chiavi

La generazione della coppia di chiavi deve essere effettuata mediante dispositivi e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.
Il sistema di generazione della coppia di chiavi deve comunque assicurare:

a. la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
b. l'equiprobabilità di generazione di tutte le coppie possibili;
c. l'identificazione del soggetto che attiva la procedura di generazione.

6. Modalità di generazione delle chiavi

1. Le chiavi di certificazione possono essere generate esclusivamente dal responsabile del servizio.

2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.

3. La generazione delle chiavi di sottoscrizione effettuata, autonomamente dal titolare, deve avvenire all'interno del dispositivo sicuro per la generazione delle firme, che deve essere rilasciato o indicato dal certificatore.

4. Il certificatore deve assicurarsi che il dispositivo sicuro per la generazione delle firme, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 29-sexies del testo unico e all'art. 9 del presente decreto.

5. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

7. Conservazione delle chiavi

1. È vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate purché ciò avvenga con modalità tali da non ridurre il livello di sicurezza.

3. Il titolare della coppia di chiavi deve:

a. conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
b. conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
c. richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso.

8. Generazione delle chiavi al di fuori del dispositivo di firma

1. Se la generazione delle chiavi avviene su un sistema diverso da quello destinato all'uso della chiave privata, il sistema di generazione deve assicurare:

a. l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura;
b. il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui verrà utilizzata.

2. Il sistema di generazione deve essere isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto contro i rischi di interferenze ed intercettazioni.

3. L'accesso al sistema deve essere controllato e ciascun utente preventivamente identificato. Ogni sessione di lavoro deve essere registrata nel giornale di controllo.

4. Prima della generazione di una nuova coppia di chiavi, l'intero sistema deve procedere alla verifica della propria configurazione, dell'autenticità ed integrità del software installato e dell'assenza di programmi non previsti dalla procedura.

9. Dispositivi sicuri e procedure per la generazione della firma

1. In aggiunta a quanto previsto all'art. 29-sexies del testo unico, la generazione della firma deve avvenire all'interno di un dispositivo sicuro di

firma, così che non sia possibile l'intercettazione della chiave privata utilizzata.

2. Il dispositivo sicuro di firma deve poter essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma.

3. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, secondo i criteri indicati all'art. 53.

4. La personalizzazione del dispositivo sicuro di firma deve almeno garantire:

a. l'acquisizione da parte del certificatore dei dati identificativi del dispositivo di firma utilizzato e la loro associazione al titolare;
b. la registrazione nel dispositivo di firma del certificato qualificato, relativo alle chiavi di sottoscrizione del titolare.

5. La personalizzazione del dispositivo sicuro di firma può prevedere, per l'utilizzo nelle procedure di verifica della firma, la registrazione, nel dispositivo di firma, del certificato elettronico relativo alla chiave pubblica del certificatore la cui corrispondente privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare.

6. La personalizzazione del dispositivo di firma è registrata nel giornale di controllo.

7. Il certificatore deve adottare, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme, procedure atte ad identificare il titolare di un dispositivo sicuro di firma e dei certificati in esso contenuti.

10. Verifica delle firme digitali

I certificatori che rilasciano certificati qualificati devono fornire ovvero indicare almeno un sistema che consenta di effettuare la verifica delle firme digitali.

11. Informazioni riguardanti i certificatori

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi del testo unico devono fornire al dipartimento le seguenti informazioni e documenti:

a. dati anagrafici ovvero denominazione o ragione sociale;
b. residenza ovvero sede legale;
c. sedi operative;

d. rappresentante legale;
e. certificati delle chiavi di certificazione;
f. piano per la sicurezza contenuto in busta sigillata;
g. manuale operativo di cui al successivo art. 38;
h. dichiarazione di impegno al rispetto delle disposizioni del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
i. dichiarazione di conformità ai requisiti previsti nel presente decreto;
l. relazione sulla struttura organizzativa;
m. copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.

2. Il Dipartimento rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), d).

3. Restano salve le disposizioni del decreto del Presidente della Repubblica 23 dicembre 1997, n. 522, e successive modificazioni, con riferimento ai compiti di certificazione e di validazione temporale del Centro nazionale per l'informatica nella pubblica amministrazione, in conformità alle disposizioni dei regolamenti previsti dall'art. 15, comma 2, della legge 15 marzo 1997, n. 59.

12. Comunicazione tra certificatore e Dipartimento

1. I certificatori che rilasciano al pubblico certificati qualificati devono attenersi alle regole emanate dal Dipartimento per realizzare un sistema di comunicazione sicuro attraverso il quale scambiare le informazioni previste dal presente decreto.

13. Generazione delle chiavi di certificazione

1. La generazione delle chiavi di certificazione deve avvenire in modo conforme a quanto previsto dal presente Titolo.

2. Per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

3. I valori contenuti nei singoli campi del certificato delle chiavi di certificazione devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

14. Generazione dei certificati qualificati

1. In aggiunta agli obblighi previsti per il certificatore dall'art. 29-bis del testo unico prima di emettere il certificato qualificato il certificatore deve:

a. accertarsi dell'autenticità della richiesta;
b. verificare il possesso della chiave privata e il corretto funzionamento della coppia di chiavi.

2. Il certificato qualificato deve essere generato con un sistema conforme a quanto previsto dall'art. 28.

3. L'emissione dei certificati qualificati deve essere registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione.

4. Il momento della generazione dei certificati deve essere attestato tramite un riferimento temporale.

15. Informazioni contenute nei certificati qualificati

1. Fatto salvo quanto previsto dall'art. 27-bis del testo unico, i certificati qualificati devono contenere almeno le seguenti informazioni:

a. codice identificativo del titolare presso il certificatore;
b. tipologia della coppia di chiavi in base all'uso cui sono destinate.

2. Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare della firma elettronica, per legittimare la sottoscrizione del documento informatico, nonché per indicare eventuali funzioni del titolare.

3. I valori contenuti nei singoli campi del certificato qualificato devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

4. Il certificatore determina il periodo di validità dei certificati qualificati in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati.

5. Il certificatore custodisce le informazioni di cui all'art. 29-bis, comma 2, lettera m) del testo unico, per un periodo non inferiore a dieci anni dalla data di scadenza o revoca del certificato qualificato.

16. Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'art. 29-septies del testo unico, il certificato qualificato deve essere revocato o sospeso dal certificatore, ove quest'ul-

timo abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma.

17. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione

1. La revoca del certificato qualificato relativo a chiavi di sottoscrizione viene effettuata dal certificatore mediante l'inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL/CSL).
2. Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione dell'aggiornamento della lista di revoca.
3. La revoca dei certificati è annotata nel giornale di controllo con la specificazione della data e dell'ora della pubblicazione della nuova lista.

18. Revoca su iniziativa del certificatore

1. Salvo i casi di motivata urgenza, il certificatore che intende revocare un certificato qualificato deve darne preventiva comunicazione al titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

19. Revoca su richiesta del titolare

1. La richiesta di revoca deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua decorrenza.

2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo di cui al successivo art. 38.

3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste al comma 2.

4. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

20. Revoca su richiesta del terzo interessato

1. La richiesta di revoca da parte del terzo interessato da cui derivano i poteri di rappresentanza del titolare deve essere inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua decorrenza.

2. Il certificatore deve notificare la revoca al titolare.

3. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

21. Sospensione dei certificati qualificati

1. La sospensione del certificato qualificato è effettuata dal certificatore attraverso l'inserimento di tale certificato in una delle liste dei certificati revocati e sospesi (CRL/CSL).

2. La sospensione dei certificati è annotata nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

22. Sospensione su iniziativa del certificatore

1. Salvo casi d'urgenza, che il certificatore è tenuto a motivare contestualmente alla comunicazione di cui al comma 2, il certificatore che intende sospendere un certificato qualificato deve darne preventiva comunicazione al titolare specificando i motivi della sospensione e la sua durata.

2. L'avvenuta sospensione del certificato qualificato deve essere tempestivamente comunicata al titolare specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.

3. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione della sospensione.

23. Sospensione su richiesta del titolare

1. La richiesta di sospensione deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua durata.

2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo.

3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal comma 2.

24. Sospensione su richiesta del terzo interessato

1. La richiesta di sospensione da parte del terzo interessato, da cui derivano i poteri di rappresentanza del titolare, deve essere inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua durata.

2. Il certificatore deve notificare la sospensione al titolare.

25. Sostituzione delle chiavi di certificazione

1. Almeno novanta giorni prima della scadenza del certificato relativo a chiavi di certificazione il certificatore deve avviare la procedura di sostituzione, generando, con le modalità previste dall'art. 13, una nuova coppia di chiavi.

2. Il certificatore deve generare un certificato relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia ed uno relativo alla vecchia chiave pubblica sottoscritto con la chiave privata della nuova coppia.

3. I certificati generati secondo quanto previsto dal comma 2 debbono essere inviati al dipartimento.

26. Revoca dei certificati relativi a chiavi di certificazione

1. La revoca del certificato relativo ad una coppia di chiavi di certificazione è consentita solo nei seguenti casi:

a. compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
b. guasto del dispositivo di firma;
c. cessazione dell'attività.

2. La revoca deve essere notificata entro ventiquattro ore al dipartimento e a tutti i titolari di certificati qualificati firmati con la chiave privata appartenente alla coppia revocata.

3. I certificati qualificati per i quali risulti compromessa la chiave privata con cui sono stati sottoscritti devono essere revocati.

27. Requisiti di sicurezza dei sistemi operativi

1. Il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati qualificati e la gestione del registro dei certificati qualificati, devono essere conformi quanto meno alle specifiche previste dalla classe ITSEC F-C2/E2 o equivalenti.

2. Il requisito di cui al comma 1 non si applica al sistema operativo dei dispositivi di firma.

28. Sistema di generazione dei certificati qualificati

1. La generazione dei certificati qualificati deve avvenire su un sistema utilizzato esclusivamente per la generazione di certificati, situato in locali adeguatamente protetti.

2. L'entrata e l'uscita dai locali protetti devono essere registrate sul giornale di controllo.

3. L'accesso ai sistemi di elaborazione deve essere consentito, limitatamente alle funzioni assegnate, esclusivamente al personale autorizzato, identificato attraverso un'opportuna procedura di riconoscimento da parte del sistema al momento di apertura di ciascuna sessione.

4. L'inizio e la fine di ciascuna sessione devono essere registrati sul giornale di controllo.

29. Accesso del pubblico ai certificati

1. Le liste dei certificati revocati e sospesi devono essere rese pubbliche.

2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico, ovvero comunicati a terzi, esclusivamente nei casi consentiti dal titolare del certificato e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.

3. Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi le consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità della firma digitale.

30. Piano per la sicurezza

1. Il certificatore deve definire un piano per la sicurezza nel quale devono essere contenuti almeno i seguenti elementi:

a. struttura generale, modalità operativa e struttura logistica;
b. descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza;
c. allocazione dei servizi e degli uffici negli immobili;
d. elenco del personale e sua allocazione negli uffici;
e. attribuzione delle responsabilità;
f. algoritmi crittografici o altri sistemi utilizzati;

g. descrizione delle procedure utilizzate nell'attività di certificazione;
h. descrizione dei dispositivi installati;
i. descrizione dei flussi di dati;
m. procedura di gestione delle copie di sicurezza dei dati;
n. procedura di gestione dei disastri;
o. analisi dei rischi;
p. descrizione delle contromisure;
q. specificazione dei controlli.

2. Fatto salvo quanto disposto al comma 3, il piano per la sicurezza, sottoscritto dal legale rappresentante del certificatore, deve essere consegnato al dipartimento in busta sigillata.

3. Le informazioni di cui al comma 1, lettere b), c) e d) devono essere consegnate al dipartimento in una busta sigillata, che verrà aperta solo in caso di contestazioni, diversa da quella nella quale è contenuto il piano per la sicurezza.

4. Il piano per la sicurezza deve attenersi quanto meno alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'art. 33, del decreto legislativo 30 giugno 2003, n. 196.

31. Giornale di controllo

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il certificatore, allorché si verificano le condizioni previste dal presente decreto.

2. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.

3. A ciascuna registrazione deve essere associato un riferimento temporale.

4. Il giornale di controllo deve essere tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

5. L'integrità del giornale di controllo deve essere verificata con frequenza almeno mensile.

6. Le registrazioni contenute nel giornale di controllo devono essere conservate per un periodo non inferiore a 10 anni.

32. Sistema di qualità del certificatore

1. Entro un anno dall'avvio dell'attività di certificazione, il certificatore deve dichiarare la conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti.

2. Il manuale della qualità deve essere depositato presso il dipartimento e reso disponibile presso il certificatore.

33. Organizzazione del personale del certificatore

1. L'organizzazione del personale addetto al servizio di certificazione deve prevedere almeno le seguenti funzioni:

a. responsabile della sicurezza;
b. responsabile della generazione e custodia delle chiavi;
c. responsabile della personalizzazione dei dispositivi di firma;
d. responsabile della generazione dei certificati;
e. responsabile della gestione del registro dei certificati;
f. responsabile della registrazione degli utenti;
g. responsabile della sicurezza dei dati;
h. responsabile della crittografia o di altro sistema utilizzato;
i. responsabile dei servizi tecnici;
l. responsabile delle verifiche e delle ispezioni (auditing);
m. responsabile del sistema di riferimento temporale.

2. È possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1 purché tra loro compatibili; sono in ogni caso compatibili tra loro le funzioni specificate nei sotto indicati raggruppamenti:

a) generazione e custodia delle chiavi, generazione dei certificati, personalizzazione dei dispositivi di firma, crittografia, sicurezza dei dati;
b) registrazione degli utenti, gestione del registro dei certificati, crittografia, sicurezza dei dati, sistema di riferimento temporale.

34. Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'art. 33 deve aver maturato una esperienza almeno quinquennale nell'analisi, progettazione e conduzione di sistemi informatici.

2. Per ogni aggiornamento apportato al sistema di certificazione deve essere previsto un apposito corso di addestramento.

35. Formato dei certificati qualificati

1. I certificati qualificati e le informazioni relative alle procedure di sospensione e di revoca devono essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni.

36. Formato della firma

1. Alla firma digitale deve essere allegato il certificato qualificato corrispondente alla chiave pubblica da utilizzare per la verifica.

37. Codice di emergenza

1. Per ciascun certificato qualificato emesso il certificatore deve fornire al titolare almeno un codice riservato, da utilizzare in caso di emergenza per confermare l'autenticità della eventuale richiesta di sospensione del certificato.

2. In caso di emergenza è possibile richiedere la sospensione immediata di un certificato qualificato utilizzando il codice previsto al comma 1. La richiesta deve essere successivamente confermata utilizzando una delle modalità previste dal certificatore.

3. Il certificatore adotta specifiche misure di sicurezza per assicurare la segretezza del codice di emergenza.

38. Manuale operativo

1. Il manuale operativo definisce le procedure applicate dal certificatore che rilascia certificati qualificati nello svolgimento della sua attività.

2. Il manuale operativo deve essere depositato presso il dipartimento e pubblicato a cura del certificatore in modo da essere consultabile per via telematica.

3. Il manuale deve contenere almeno le seguenti informazioni:

a. dati identificativi del certificatore;
b. dati identificativi della versione del manuale operativo;

c. responsabile del manuale operativo;
d. definizione degli obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme;
e. definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f. indirizzo del sito web del certificatore ove sono pubblicate le tariffe;
g. modalità di identificazione e registrazione degli utenti;
h. modalità di generazione delle chiavi per la creazione e la verifica della firma;
i. modalità di emissione dei certificati;
l. modalità con cui viene espletato quanto previsto all'art. 27-bis, comma 1, lettera a) del testo unico;
m. modalità di sospensione e revoca dei certificati;
n. modalità di sostituzione delle chiavi;
o. modalità di gestione del registro dei certificati;
p. modalità di accesso al registro dei certificati;
q. modalità di protezione della riservatezza;
r. modalità per l'apposizione e la definizione del riferimento temporale;
s. modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 10, comma 1;
t. modalità operative per la generazione della firma digitale.

39. Riferimenti temporali opponibili ai terzi

1. I riferimenti temporali realizzati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 14, comma 2, del testo unico.

2. I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 14, comma 2, del testo unico.

3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al D.M. 30 novembre 1993, n. 591 del Ministro dell'industria, del commercio e dell'artigianato, con una differenza non superiore ad un minuto primo.

4. Le pubbliche amministrazioni possono anche utilizzare come sistemi di validazione temporale:

a. il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272;
b. il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti;
c. il riferimento temporale ottenuto attraverso l'utilizzo di posta certificata ai sensi dell'art. 14 del testo unico.

TITOLO III
Ulteriori regole per i certificatori accreditati

40. Obblighi per i certificatori accreditati

1. Il certificatore deve generare un certificato qualificato per ciascuna delle chiavi di firma elettronica avanzata utilizzate dal dipartimento per la sottoscrizione dell'elenco pubblico dei certificatori e pubblicarlo nel proprio registro dei certificati.

2. Il certificatore garantisce l'interoperabilità del prodotto di verifica di cui all'art. 10 ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative.

3. Il certificatore deve mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiavi di certificazione di cui all'art. 41, comma 1, lettera f), che deve rendere accessibile per via telematica.

4. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 28, comma 1 del testo unico, devono svolgere la propria attività in conformità con quanto previsto dalle regole per il riconoscimento e la verifica del documento elettronico.

41. Elenco pubblico dei certificatori accreditati

1. L'elenco pubblico dei certificatori accreditati tenuto dal dipartimento ai sensi del testo unico, contiene per ogni certificatore accreditato le seguenti informazioni:

a. denominazione;

b. sede legale;
c. rappresentante legale;
d. nome X.500;
e. indirizzo internet;
f. lista dei certificati delle chiavi di certificazione;
g. manuale operativo;
h. data di accreditamento volontario;
i. data di cessazione ed eventuale certificatore sostitutivo.

2. L'elenco pubblico è sottoscritto e reso disponibile per via telematica dal dipartimento.

3. Il dipartimento provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione e a rendere la stessa disponibile ai certificatori per la pubblicazione ai sensi dell'art. 40, comma 3.

4. L'elenco pubblico è sottoscritto dal Capo del dipartimento o dal dirigente da lui designato, mediante una firma elettronica avanzata, generata mediante un dispositivo sicuro per la creazione di una firma.

5. Sulla Gazzetta Ufficiale è dato avviso:

a. della costituzione dell'elenco di cui al comma 4;
b. dell'indicazione del soggetto preposto alla sottoscrizione dell'elenco pubblico di cui al comma 4;
c. del valore dei codici identificativi delle chiavi pubbliche relative alle coppie di chiavi utilizzate per la sottoscrizione dell'elenco pubblico, generati attraverso gli algoritmi dedicated hash-function 3, corrispondente alla funzione SHA- 1 e dedicated hash-function 1, corrispondente alla funzione RIPEMD-160, definiti nella norma ISO/IEC 10118-3:1998;
d. con almeno novanta giorni di preavviso, della scadenza delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico;
e. della revoca delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico sopravvenute per ragioni di sicurezza, ovvero a seguito di sostituzione dei soggetti designati ai sensi della lettera b).

6. Fino alla certificazione delle chiavi da parte del dipartimento ai sensi dell'art. 29-quinquies del testo unico si utilizzano, per la sottoscrizione dell'elenco pubblico, le chiavi di sottoscrizione di soggetti designati dal Ministro per l'innovazione e le tecnologie.

42. Rappresentazione del documento informatico

1. Il certificatore deve indicare nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per ottemperare a quanto prescritto dall'art. 3, comma 3.

43. Limitazioni d'uso

1. Il certificatore, su richiesta del titolare o del terzo interessato, è tenuto a inserire nel certificato qualificato eventuali limitazioni d'uso.

TITOLO IV
REGOLE PER LA VALIDAZIONE TEMPORALE E PER LA PROTEZIONE DEI DOCUMENTI INFORMATICI

44. Validazione temporale

1. Una evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi.

2. Le marche temporali sono generate da un apposito sistema elettronico sicuro in grado di:

a. mantenere la data e l'ora conformemente a quanto richiesto dal presente decreto;
b. generare la struttura di dati secondo quanto specificato negli articoli 45 e 48;
c. sottoscrivere digitalmente la struttura di dati di cui alla lettera b).

45. Informazioni contenute nella marca temporale

1. Una marca temporale deve contenere almeno le seguenti informazioni:

a. identificativo dell'emittente;
b. numero di serie della marca temporale;
c. algoritmo di sottoscrizione della marca temporale;
d. identificativo del certificato relativo alla chiave di verifica della marca;
e. data ed ora di generazione della marca;

f. identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;

g. valore dell'impronta dell'evidenza informatica.

2. La marca temporale può inoltre contenere un identificatore dell'oggetto a cui appartiene l'impronta di cui al comma 1, lettera g).

46. Chiavi di marcatura temporale

1. Ogni coppia di chiavi utilizzata per la validazione temporale deve essere univocamente associata ad un sistema di validazione temporale.

2. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale debbono essere sostituite ed un nuovo certificato deve essere emesso dopo non più di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.

3. Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale debbono essere utilizzate chiavi di certificazione appositamente generate.

4. Le chiavi di certificazione e di marcatura temporale possono essere generate esclusivamente dai responsabili dei rispettivi servizi.

47. Gestione dei certificati e delle chiavi

1. Alle chiavi di certificazione utilizzate, ai sensi dell'art. 46, comma 3, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.

2. I certificati relativi ad una coppia di chiavi di marcatura temporale, oltre ad essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni, devono contenere l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

48. Precisione dei sistemi di validazione temporale

1. L'ora assegnata ad una marca temporale deve corrispondere, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al D.M. 30 novembre 1993, n. 591 del Ministro dell'industria, del commercio e dell'artigianato, al momento della sua generazione.

2. La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato (UTC).

49. Sicurezza dei sistemi di validazione temporale

1. Ogni sistema di validazione temporale deve produrre un registro operativo su di un supporto non riscrivibile nel quale sono automaticamente registrati gli eventi per i quali tale registrazione è richiesta dal presente decreto.

2. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento dell'apparato in modo da renderlo incompatibile con i requisiti del presente decreto, ed in particolare con quello di cui all'art. 48, comma 1, deve essere annotato sul registro operativo e causare il blocco del sistema.

3. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.

4. La conformità ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo criteri di sicurezza almeno equivalenti a quelli previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC, o dal livello EAL 3 della norma ISO/IEC 15408 o superiori. Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

50. Registrazione delle marche generate

1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a cinque anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.

2. La marca temporale è valida per l'intero periodo di conservazione a cura del fornitore del servizio.

51. Richiesta di validazione temporale

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'inoltro della richiesta di validazione temporale.

2. La richiesta deve contenere l'evidenza informatica alla quale le marche temporali debbono fare riferimento.

3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash previste dal manuale operativo. Debbono essere comunque accettate le funzioni di hash basate sugli algoritmi dedicated hash-function 3, corrispondente alla funzione SHA-1 e dedicated hash-function 1, corrispondente alla funzione RIPEMD-160, definiti nella norma ISO/IEC 10118-3:1998.

4. Il certificatore ha facoltà di implementare il sistema di validazione temporale in modo che sia possibile richiedere l'emissione di più marche temporali per la stessa evidenza informatica. In tal caso debbono essere restituite marche temporali generate con chiavi diverse.

5. La generazione delle marche temporali deve garantire un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

52. Estensione della validità del documento informatico

1. La validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una marca temporale.

TITOLO V
Disposizioni finali e transitorie

53. Norme transitorie

1. In attesa della pubblicazione degli algoritmi per la generazione e verifica della firma digitale secondo quanto previsto dall'art. 3, i certificatori accreditati ai sensi dell'art. 28 del testo unico, devono utilizzare l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 1024 bit.

2. In attesa della pubblicazione delle funzioni di hash secondo quanto previsto dall'art. 3, i certificatori accreditati ai sensi dell'art. 28 del testo unico devono utilizzare uno dei seguenti algoritmi, definiti nella norma ISO/IEC 10118-3:1998 e successive evoluzioni:

a. dedicated hash-function 3, corrispondente alla funzione SHA-1;
b. dedicated hash-function 1, corrispondente alla funzione RIPEMD-160.

3. In attesa che la Commissione europea, secondo la procedura di cui all'art. 9 della direttiva 1999/93/CE, indichi i livelli di valutazione relativamente alla certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma prevista dall'art. 10 del decreto legislativo 23 gennaio 2002, n. 10, tale certificazione è effettuata secondo criteri non inferiori a quelli previsti dal livello di valutazione E3 e robustezza HIGH dell'ITSEC, o dal livello EAL 4 della norma ISO/IEC 15408 o superiori. Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

4. Il dipartimento disciplina con circolare il riconoscimento e la verifica del documento elettronico; fino all'emanazione della prima circolare continueranno ad applicarsi le regole vigenti adottate dal Centro nazionale per l'informatica nella pubblica amministrazione.

54. Abrogazioni

1. Dall'entrata in vigore del presente decreto è abrogato il decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, recante le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, pubblicato nella Gazzetta Ufficiale 15 aprile 1999, n. 87.

NORME TRANSITORIE

Nell'allegato al DPCM 8 febbraio 1999, abrogato dal DPCM 13 gennaio 2004 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici") all'art. 63 viene introdotta la seguente procedura "transitoria": "Le disposizioni che richiedono verifiche secondo i criteri previsti da livelli di valutazione ITSEC non si applicano nei diciotto mesi successivi alla data di entrata in vigore delle presenti regole tecniche. Durante il periodo transitorio, il fornitore o il certificatore, secondo le rispettive competenze, devono tuttavia attestare, mediante autodichiarazione, la rispondenza dei dispositivi ai requisiti di sicurezza imposti dalle suddette disposizioni." Il DPCM del 7 dicembre 2000 sposta il termine al 28 marzo 2001, quello del 20 aprile 2001 al 30 settembre 2001, mentre quello del 3 ottobre 2001 lo proroga fino al 31 maggio 2002. Il termine è stato ulteriormente prorogato dal DPCM 30 ottobre 2003.

Estratto dal Decreto del Presidente del Consiglio dei Ministri 7 dicembre 2000

Proroga del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al D.P.C.M. 8 febbraio 1999

Articolo unico. 1. Il periodo di diciotto mesi successivi alla data di entrata in vigore delle regole tecniche, introdotte dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, è differito al 28 marzo 2001.

Estratto dal Decreto del Presidente del Consiglio dei Ministri 20 aprile 2001

Differimento del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al D.P.C.M. 8 febbraio 1999

Articolo unico. 1. Il periodo di diciotto mesi successivi alla data di entrata in vigore delle regole tecniche, introdotte dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, è differito al 30 settembre 2001.

Estratto dal Decreto del Presidente del Consiglio dei Ministri 3 ottobre 2001

Differimento del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al D.P.C.M. 8 febbraio 1999

1. 1. Il termine stabilito dall'art. 63 delle regole tecniche stabilite dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato nella Gazzetta Ufficiale n. 87 del 15 aprile 1999, già differito al 30 settembre 2001, è ulteriormente differito al 31 maggio 2002.

Estratto dal Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003

Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10

Art. 13

(Norme transitorie e finali)

3. Per le valutazioni dei dispositivi di firma già effettuate, ai sensi delle vigenti regole tecniche, prima dell'entrata in vigore del presente decreto da centri di valutazione rispondenti ai requisiti di cui al presente decreto, ciascun LVS invia all'organismo di certificazione il rapporto formale di valutazione. L'organismo di certificazione procede ai sensi dei commi 6 e seguenti dell'art. 9.

4. Per un periodo di nove mesi decorrente dall'entrata in vigore del presente decreto, i certificatori di firma elettronica attestano la rispondenza dei propri prodotti e dispositivi di firma elettronica ai requisiti di sicurezza previsti dalla vigente normativa mediante autodichiarazione. Decorso il periodo indicato, si ricorre alla certificazione ai sensi del presente decreto, come prescritto dall'art. 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

5. Le autodichiarazioni rese ai sensi dei decreti del Presidente del Consiglio dei Ministri del 7 dicembre 2000, del 20 aprile 2001 e del 3 ottobre 2001, continuano a spiegare ininterrottamente i propri effetti fino al termine del periodo di cui al comma 4.

NORME ATTUATIVE DEL CNIPA

Scheda illustrativa della Circolare CNIPA n. 46 del 27 gennaio 2005

Attuazione delle disposizioni di cui all'articolo 41 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004: codici identificativi della chiave pubblica relativa alle coppie di chiavi utilizzate dal Presidente del Centro nazionale per l'informatica nella pubblica amministrazione per la sottoscrizione dell'elenco pubblico

La Circolare n. 46 del CNIPA dà attuazione alle disposizioni dell'art. 41 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicando i codici identificativi della chiave pubblica relativa alle coppie di chiavi utilizzate dal Presidente del CNIPA, dott. Livio Zoffoli, per la sottoscrizione dell'elenco pubblico.
Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione esegue tale adempimento in base alle disposizioni del decreto 2 luglio 2004 del Ministro per l'Innovazione e le Tecnologie: «Competenza in materia di certificatori di firma elettronica», ove è previsto che il CNIPA provveda alla tenuta dell'elenco pubblico dei certificatori e curi gli adempimenti connessi (previsti dal decreto legislativo 23 gennaio 2002, n. 10, dall'art. 27 e seguenti del decreto del Presidente della Repubblica n. 445 del 2000 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).
I codici in parola, costituiti dall'impronta del certificato della suddetta chiave pubblica, generata impiegando ambedue le funzioni di hash RIPEMD-160 e SHA-1, sono:

a. 6482 F960 DC58 7DF5 BCA9 9E59 4B39 8019 05C5 56B0, ottenuto utilizzando l'algoritmo ISO/IEC 10118-3: 1998 Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160;
b. F758 2B22 3891 3258 A5F3 4FFF A06A 5A26 8997 732B, ottenuto utilizzando l'algoritmo ISO/IEC 10118-3: 1998 Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

Tale certificato è stato emesso dal CNIPA il 28 dicembre 2004 con il numero di serie 41D1 2C19.

Scheda illustrativa della Deliberazione CNIPA n. 4 del 17 febbraio 2005

Regole per il riconoscimento e la verifica del documento informatico

La Deliberazione CNIPA n. 4 del 17 febbraio 2005 stabilisce, ai sensi dell'art. 40, comma 4 delle regole tecniche, le regole per il riconoscimento e la verifica del documento informatico cui i certificatori accreditati devono attenersi al fine di ottenere e mantenere il riconoscimento di cui all'Articolo 28, comma 1 del testo unico.

Titolo I

Disposizioni che definiscono le regole, l'ambito di applicazione e il contenuto.

Titolo II

Disposizioni che definiscono il formato dei certificati qualificati e le informazioni che in essi devono essere contenute.

Titolo III

Disposizioni che definiscono il formato dei certificati elettronici di certificazione e le informazioni che in essi devono essere contenute, generati ai sensi dell'Articolo 13, comma 2, delle regole tecniche, e il formato dei certificati elettronici di marcatura temporale e le informazioni che in essi devono essere contenute.

Titolo IV

Disposizioni che definiscono il formato e le informazioni che devono essere contenute nelle marche temporali utilizzate dai sistemi di validazione temporale dei documenti, così come definiti nel titolo IV delle regole tecniche.

Titolo V

Disposizioni che definiscono i formati e le modalità di accesso alle informazioni sulla revoca e la sospensione dei certificati, ai sensi dell'Articolo 29, comma 1, delle regole tecniche.

Titolo VI

Disposizioni che definiscono i formati delle buste crittografiche destinate a contenere gli oggetti sottoscritti con firma digitale.

Titolo VII

Disposizioni che definiscono i requisiti delle applicazioni di verifica della firma digitale di cui all'Articolo 10 delle regole tecniche.

Scheda illustrativa della Circolare CNIPA n. 48 del 6 settembre 2005

Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445

La Circolare CNIPA n. 48 indica le modalità per presentare la domanda di iscrizione, per soggetti pubblici o privati, nell'elenco pubblico dei certificatori di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – art. 28, comma 1 («Testo unico» delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e come sostituito dall'art. 13 del decreto del Presidente della Repubblica 7 aprile 2003, n. 137).

Domanda di iscrizione

La domanda di accreditamento deve indicare la denominazione o la ragione sociale, la sede legale, le sedi operative, il/i rappresentante/i legale/i, l'elenco dei documenti allegati e i recapiti di un referente. Deve, inoltre, essere sottoscritta dal legale rappresentante della pubblica amministrazione o della società richiedente e consegnata tramite servizio pubblico o privato oppure a mano, nelle ore d'ufficio dei giorni feriali, al CNIPA.

Requisiti soggetti privati

I soggetti privati devono dimostrare il possesso dei requisiti previsti dagli articoli 27 e 28, comma 3, del testo unico e dall'art. 11, comma 1, articoli 30, 34 e 38 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004. A tal fine dovranno allegare alla domanda: copia autentica dell'atto costitutivo della società; copia dello statuto sociale aggiornato e certificato

di iscrizione nel registro delle imprese con dicitura antimafia, rilasciati in data non anteriore a novanta giorni rispetto a quella di presentazione della domanda; dichiarazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile, di data non anteriore a trenta giorni, attestante l'entità del capitale sociale versato e l'ammontare e la composizione del patrimonio netto; situazione patrimoniale, predisposta e approvata dall'organo amministrativo, (non anteriore a centottanta giorni e solo per le società già operative) e una relazione sulla stessa da parte dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile. Oppure una documentazione equivalente per le società costituite all'estero ed aventi sede in Italia (art. 33 del Testo unico). Tra gli allegati deve inoltre comparire l'elenco nominativo dei rappresentanti legali, dei componenti dell'organo di amministrazione e di controllo, e di eventuali altri soggetti preposti all'amministrazione, con l'indicazione dei relativi poteri e dichiarazione del possesso dei requisiti di cui all'art. 28 del testo unico. Le firme apposte su tale documentazione devono essere legalizzate con le modalità previste dal testo unico. I soggetti iscritti all'albo (art. 13 del decreto legislativo 1° settembre 1993, n. 385) per dimostrare il possesso dei requisiti potranno ricorrere a una dichiarazione sostitutiva (art. 46 del Testo unico) del legale rappresentante, attestante l'iscrizione all'albo in data anteriore a quella di presentazione della domanda. Va poi allegata copia della polizza assicurativa (o certificato provvisorio impegnativo) per la copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali; copia dell'ultimo bilancio e relativa certificazione per società costituite da più di un anno; dichiarazione del presidente della società con la composizione dell'azionariato e l'indicazione dei soggetti partecipanti, in forma diretta o indiretta, al capitale sociale in misura superiore al 5%.

Requisiti soggetti privati e pubbliche amministrazioni

I soggetti privati e le pubbliche amministrazioni dovranno inserire a corredo della domanda una copia del piano per la sicurezza (sottoscritto e siglato in ogni foglio) e copia del manuale operativo sottoscritti da soggetto munito di potere di firma; una relazione sulla struttura organizzativa, a firma del legale rappresentante; dichiarazione per consentire l'accesso di incaricati del CNIPA nelle strutture dedicate alle operazioni di certificazione, al fine di poter verificare la permanenza dei requisiti tecnico-organizzativi; dichiarazione di impegno: a rispettare quanto prescritto dall'art. 53, comma 4, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 e succes-

sive modificazioni; a comunicare al CNIPA le caratteristiche dei «dispositivi sicuri per la creazione della firma» che si intende fornire e ogni eventuale variazione intervenuta per una nuova valutazione dei requisiti o richiesta di ulteriore documentazione da parte del CNIPA. Alla domanda va anche allegata una dichiarazione tecnica (art. 29-bis, comma 2, lettera f, del testo unico e dell'art. 11, comma 1, lettera i, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004) contenente: algoritmi di generazione e di verifica delle firme utilizzati e supportati dal certificatore; algoritmi di hash utilizzati e supportati dal certificatore; garanzie relative al sistema di generazione e lunghezza delle chiavi; informazioni contenute e formato dei certificati; modalità di accesso alle informazioni di revoca e di sospensione dei certificati; modalità per soddisfare la verifica dell'unicità della chiave pubblica; caratteristiche del sistema di generazione dei certificati; modalità di attuazione della copia del registro dei certificati e di tenuta del giornale di controllo; descrizione del sistema di validazione temporale adottato; impegno ad adottare ogni opportuna misura tecnico-organizzativa volta a garantire il rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni. Nella dichiarazione tecnica possono non essere riportate informazioni soggette a particolari ragioni di riservatezza. Alla domanda deve essere infine allegato un supporto informatico contenente copia del manuale operativo e della dichiarazione tecnica, predisposta utilizzando un sistema di elaborazione testi di larga diffusione. Il CNIPA, si riserva, a norma dell'art. 28, comma 5 del testo unico, di richiedere integrazioni e di effettuare le opportune verifiche su quanto dichiarato. Il manuale operativo va strutturato in modo tale da essere integralmente consultabile per via telematica (art. 38, comma 2, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004) e deve contenere, quanto meno, le informazioni previste dal comma 3 dello stesso art. 38. Il piano per la sicurezza, contenente almeno le informazioni previste nell'art. 30 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, deve essere consegnato seguendo le modalità dell'art. stesso.
La domanda e la documentazione da allegare possono essere predisposte, ove possibile, in formato elettronico, sottoscritte con firma digitale e inviate alla casella di posta elettronica certificata CNIPAdir@cert.CNIPA.it.

Valutazione della documentazione da parte del CNIPA

L'istruttoria relativa alle domande e la valutazione della documentazione prodotta sono effettuate dal CNIPA ai sensi del decreto 2 luglio 2004, recante: «Competenza in materia di certificatori di firma elettronica». Al termine

dell'istruttoria, il CNIPA, sulla base della documentazione pervenuta, accoglie o rigetta la domanda, ovvero, se necessario, dispone un'integrazione dell'istruttoria. Nel caso in cui alla domanda non sia allegata tutta la documentazione prevista dalla presente circolare, il richiedente potrà presentare – contestualmente alla domanda stessa – richiesta di sospensione dei termini previsti dall'art. 28, comma 4, del Testo unico. Il soggetto la cui domanda sia stata oggetto di un provvedimento di reiezione non può presentare una nuova istanza se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente.

Scheda illustrativa della Deliberazione CNIPA n. 34 del 18 maggio 2006

Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML

La Deliberazione CNIPA n. 34 del 18 maggio 2006 emana le regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML.
Detta Deliberazione fa riferimento al profilo, al formato e alla struttura dei certificati definiti nella deliberazione CNIPA n. 4 del 17 febbraio 2005. I certificatori accreditati ai sensi dell'articolo 29, comma 1, del decreto legislativo 7 marzo 2005, n. 82, che rilasciano strumenti per la sottoscrizione nei formati previsti dalla presente deliberazione, devono fornire, ovvero indicare (art. 10, comma 1, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004) almeno un sistema che consenta di effettuare la verifica della sottoscrizione stessa.
Le regole tecniche vengono sinteticamente riportate nel seguente allegato.

Scheda dell'allegato alla deliberazione CNIPA n. 34/2006

Le buste crittografiche devono essere, ove non diversamente indicato, conformi alla specifica RFC 3275.

Tipologie di firme e algoritmi

Le XML Signature si presentano in tre forme base di modalità di imbustamento:

– Enveloped
  http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloped

– Enveloping
  http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloping

– Detached
  http://www.w3.org/TR/xmldsig-core/#def-SignatureDetached
  Le applicazioni di apposizione della firma possono realizzare le buste crittografiche in una qualsiasi delle modalità consentite. Conseguentemente, le applicazioni di verifica devono essere in grado di verificare le firme in una qualsiasi di queste modalità.
  La funzione di *hash* che le applicazioni di firma devono specificare e, quindi, applicare all'oggetto da firmare è la funzione SHA-1 (ISO/IEC 10118-3:1998).

L'URI che deve essere indicata nell'attributo *Algorithm* dell'elemento *DigestMethod* è:

– http://www.w3.org/2000/09/xmldsig#sha1
  Le applicazioni di verifica devono gestire almeno questo algoritmo.
  L'algoritmo per la generazione e la validazione della firma digitale (*SignatureValue*) che le applicazioni di firma devono specificare e, quindi, applicare all'elemento *SignedInfo* è l'algoritmo RSA-SHA1.
  L'URI che deve essere indicata nell'attributo *Algorithm* dell'elemento *SignatureMethod* è:
– http://www.w3.org/2000/09/xmldsig#rsa-sha1
  Le applicazioni di verifica devono gestire almeno questo algoritmo.
  L'applicazione di firma può usare quale algoritmo di canonicalizzazione dell'elemento *SignedInfo* uno tra quelli identificati dalle URI seguenti:
– http://www.w3.org/TR/2001/REC-xml-c14n-20010315
– http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComment

Questa URI deve essere riportata nell'attributo *Algorithm* dell'elemento *CanonicalizationMethod.*
Le applicazioni di verifica devono gestire almeno questi algoritmi di canonicalizzazione.

Con riferimento alla specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES le applicazioni di verifica devono gestire i formati XAdES-BES e XAdES-T.

Associazione di una Marca Temporale alla firma

La marca temporale è ottenuta inviando un'impronta di un documento ad un TSP che firma con un certificato emesso da una TSA (Time Stamping

Authority) di cui ha disponibilità un certificatore accreditato iscritto nell'elenco pubblico tenuto dal CNIPA.
Il risultato (TimeStampToken) è un oggetto di tipo *signed-data* ottenuto firmando l'hash + alcune altre informazioni tra cui la data e ora secondo la specifica RFC 3161.
Si prende in considerazione la marcatura della sola firma. Questa viene inserita tra gli attributi qualificati non firmati. Il formato che descrive il requisito è lo XAdES-T.

Firme multiple

La realizzazione delle firme multiple congiunte (altrimenti dette contestuali o parallele) è caratterizzata dal fatto che esse sono apposte in modo indipendente sugli stessi dati di partenza.
Nel caso particolare di XML Signature possiamo evidenziare che:

– all'elemento *Signature* corrisponde una sola firma e quindi un solo firmatario; gli elementi *Reference* che individuano il documento, ovvero i documenti, firmati, sono contenuti nell'elemento *Signature* e contengono anche il DigestValue di ciascuno di essi. L'attributo *Signature ID* deve essere valorizzato e deve essere univoco per ciascun firmatario.

Se la busta di partenza contiene una firma *enveloping,* le firme successive devono essere apposte in modalità *detached* facendo riferimento ai dati firmati nella busta di partenza presenti nel *tag object*.
Se la busta di partenza contiene una firma XML in modalità *detached,* le firme seguenti devono essere apposte utilizzando ancora la modalità *detached* facendo riferimento ai dati referenziati dal primo firmatario.
Se la busta crittografica di partenza contiene una firma XML in modalità *enveloped,* le firme seguenti devono essere apposte utilizzando ancora la modalità *enveloped*.

Controfirme

Le controfirme devono utilizzare quando stabilito dalla specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES.

INIZIATIVE IN CORSO E NUOVI SVILUPPI

Le norme tecniche sulla firma digitale fin dal 1999 prescrivono che la firma digitale debba essere generata utilizzando uno specifico formato, costituito dalla busta crittografica PKCS#7, noto come file "p7m". Questa previsione ha consentito di ottenere il libero scambio dei documenti informatici sottoscritti con firma digitale in quanto è possibile verificare le firme stesse utilizzando diversi applicativi di verifica a prescindere dal certificatore che ha rilasciato il dispositivo utilizzato per generare la firma. Nel tempo ci si è resi conto che sarebbe stato auspicabile, per fornire ulteriore slancio alla diffusione del documento informatico, poter individuare ulteriori formati di firma che, per caratteristiche intrinseche potessero incontrare l'interesse delle amministrazioni, e non solo, per informatizzare flussi informativi e scambi documentali. A tale scopo la deliberazione CNIPA n. 4/2005 del 17 febbraio 2005 ha previsto che il CNIPA possa stabilire ulteriori formati di firma (cfr. art. 12, comma 8) conformi a specifiche pubbliche riconosciute a livello nazionale o internazionale. Il comma 9 dello stesso articolo contempla la possibilità per il CNIPA di sottoscrivere specifici protocolli d'intesa volti a rendere disponibili ulteriori formati di firma. In questo caso si tratta di formati di firma proprietari, che sono resi noti a cura del legittimo proprietario che si assume, con la sottoscrizione, numerosi impegni, fra cui rendere disponibile per uso gratuito un prodotto per gestire, visualizzare e sottoscrivere i documenti informatici utilizzando le smart card fornite dai certificatori accreditati. Fra gli altri obblighi assunti si ricorda l'impegno a rendere disponibili gratuitamente tutte le specifiche tecniche necessarie a chi intendesse sviluppare prodotti che gestiscono il formato oggetto del protocollo d'intesa.

In breve, attraverso la deliberazione CNIPA n. 4/2005, sarà possibile fruire di ulteriori formati di firma. È fondamentale che, nel caso dei formati proprietari previsti dal comma 9, tutte le amministrazioni che li vorranno utilizzare (si ricorda che trattasi di facoltà, l'unico formato obbligatorio è il PKCS#7) ne informino il CNIPA in modo che, nel caso insorgessero problemi con il firmatario del protocollo d'intesa, il CNIPA possa informare tempestivamente le amministrazioni interessate.

A seguito della deliberazione n. 4/2005, il 16 febbraio 2006 è stato sottoscritto un primo protocollo d'intesa volto a rendere disponibile il formato di firma digitale definito nelle specifiche PDF (Portable Document Format) proposto dalla società Adobe.