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.

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 e' 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 tecnologica, dello sviluppo della societa' dell'informazione, nonche' 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 Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, CE attuata con decreto legislativo 23 novembre 2000, n. 427;

Decreta:

Titolo I
DISPOSIZIONI GENERALI

Art. 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 puo' essere elaborata da una procedura informatica;

g) riferimento temporale, informazione, contenente la data e l'ora, che viene associata ad uno o piu' documenti informatici;

h) validazione temporale, il risultato della procedura informatica, con cui si attribuisce, ad uno o piu' documenti informatici, un riferimento temporale opponibile ai terzi;

i) marca temporale, un'evidenza informatica che consente la validazione temporale.

Art. 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 conformita' alle norme nazionali di recepimento della direttiva 1999/93/CE, e' 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

Art. 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 funzionalita' che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Art. 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 puo' 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 piu' 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 e' 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 finalita' 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.

Art. 5.
Generazione delle chiavi

1. 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'unicita' e la robustezza della coppia generata, nonche' la segretezza della chiave privata.
2. 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'equiprobabilita' di generazione di tutte le coppie possibili;
    c) l'identificazione del soggetto che attiva la procedura di generazione.

Art. 6.
Modalita' 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 e' tenuto ad utilizzare esclusivamente il dispositivo fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art. 7.
Conservazione delle chiavi

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

2. Per fini particolari di sicurezza, e' consentito che le chiavi di certificazione vengano esportate purche' cio' avvenga con modalita' 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'integrita' 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.

Art. 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'impossibilita' 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 verra' utilizzata.

2. Il sistema di generazione deve essere isolato, dedicato esclusivamente a questa attivita' 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'autenticita' ed integrita' del software installato e dell'assenza di programmi non previsti dalla procedura.

Art. 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, cosi' 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 puo' 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 e' stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare;

6. La personalizzazione del dispositivo di firma e' 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.

Art. 10.
Verifica delle firme digitali

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

Art. 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 conformita' ai requisiti previsti nel presente decreto;

l) relazione sulla struttura organizzativa;

m) copia di una polizza assicurativa di copertura dei rischi dell'attivita' 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 nelle pubbliche amministrazioni, in conformita' alle disposizioni dei regolamenti previsti dall'art. 15, comma 2, della legge 15 marzo 1997, n. 59.

Art. 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.

Art. 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.

Art. 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'autenticita' 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.

Art. 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, nonche' 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 validita' 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.

Art. 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'ultimo abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma.

Art. 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 e' annotata nel giornale di controllo con la specificazione della data e dell'ora della pubblicazione della nuova lista.

Art. 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 nonche' la data e l'ora a partire dalla quale la revoca e' efficace.

Art. 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 modalita' di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo di cui al successivo art. 38.

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

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

Art. 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 possibilita' di accertare in tempo utile l'autenticita' della richiesta, procede alla sospensione del certificato.

Art. 21.
Sospensione dei certificati qualificati

1. La sospensione del certificato qualificato e' 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 e' annotata nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

Art. 22.
Sospensione su iniziativa del certificatore

1. Salvo casi d'urgenza, che il certificatore e' 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 e' causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione della sospensione.

Art. 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 modalita' di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo.
3. Il certificatore deve verificare l'autenticita' della richiesta e procedere alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalita' previste dal comma 2.

Art. 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.

Art. 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 modalita' 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.

Art. 26.
Revoca dei certificati relativi a chiavi di certificazione

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

a) compromissione della chiave privata, intesa come diminuita affidabilita' nelle caratteristiche di sicurezza della chiave privata;

b) guasto del dispositivo di firma;

c) cessazione dell'attivita'.

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.

Art. 27.
Requisiti di sicurezza dei sistemi operativi

1. Il sistema operativo dei sistemi di elaborazione utilizzati nelle attivita' 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.

Art. 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 deve essere registrata 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 registrate sul giornale di controllo.

Art. 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, nonche' i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi le consulta per le sole finalita' di applicazione delle norme che disciplinano la verifica e la validita' della firma digitale.

Art. 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, modalita' 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 responsabilita';

f) algoritmi crittografici o altri sistemi utilizzati;

g) descrizione delle procedure utilizzate nell'attivita' di certificazione;

h) descrizione dei dispositivi installati;

i) descrizione dei flussi di dati;

l) procedura di gestione delle copie di sicurezza dei dati;

m) procedura di gestione dei disastri;

n) analisi dei rischi;

o) descrizione delle contromisure;

p) 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 verra' aperta solo in caso di contestazioni, diversa da quella nella quale e' 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.

Art. 31.
Giornale di controllo

1. Il giornale di controllo e' costituito dall'insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il certificatore, allorche' 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'autenticita' delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

5. L'integrita' 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.

Art. 32.
Sistema di qualita' del certificatore

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

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

Art. 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. E' possibile attribuire al medesimo soggetto piu' funzioni tra quelle previste dal comma 1 purche' 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.

Art. 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.

Art. 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.

Art. 36.

Formato della firma

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

Art. 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'autenticita' della eventuale richiesta di sospensione del certificato.
2. In caso di emergenza e' 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 modalita' previste dal certificatore.
3. Il certificatore adotta specifiche misure di sicurezza per assicurare la segretezza del codice di emergenza.

Art. 38.
Manuale operativo

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

Art. 39.
Riferimenti temporali opponibili ai terzi

1. I riferimenti temporali realizzati in conformita' 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 decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, 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 conformita' 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

Art. 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'interoperabilita' 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 attivita' in conformita' con quanto previsto dalle regole per il riconoscimento e la verifica del documento elettronico.

Art. 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 e' 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 e' 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 e' 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.

Art. 42.
Rappresentazione del documento informatico

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

Art. 43.
Limitazioni d'uso

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

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

Art. 44.

Validazione temporale

1. Una evidenza informatica e' 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).

Art. 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 puo' inoltre contenere un identificatore dell'oggetto a cui appartiene l'impronta di cui al comma 1, lettera g).

Art. 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 piu' di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validita' 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.

Art. 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 1'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 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 decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, al momento della sua generazione.
2. La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato (UTC).

Art. 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 e' 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 puo' essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.
4. La conformita' 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.

Art. 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 e' valida per l'intero periodo di conservazione a cura del fornitore del servizio.

Art. 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 puo' essere sostituita da una o piu' 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 facolta' di implementare il sistema di validazione temporale in modo che sia possibile richiedere l'emissione di piu' 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.

Art. 52.
Estensione della validita' del documento informatico

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

Titolo V
DISPOSIZIONI FINALI E TRANSITORIE

Art. 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 e' 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 dall'Autorita' per l'informatica nelle pubbliche amministrazioni.

Art. 54.
Abrogazioni

1. Dall'entrata in vigore del presente decreto e' 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.

Roma, 13 gennaio 2004