D.P.C.M. 30 marzo 2009 .

Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

Pubblicato nella Gazz. Uff. 6 giugno 2009, n. 129.

IL PRESIDENTE

DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il codice dell'amministrazione digitale e, in particolare, la sezione II, che disciplina le firme elettroniche ed i certificatori, e l'art. 71, comma 1;

Visto il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante codice in materia di protezione dei dati personali;

Visto il decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, 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 27 aprile 2004, n. 98;

Visto il decreto del Presidente della Repubblica in data 7 maggio 2008, con il quale l'on. prof. Renato Brunetta è stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei Ministri dell'8 maggio 2008, con il quale al predetto Ministro senza portafoglio è stato conferito l'incarico per la pubblica amministrazione e l'innovazione;

Visto il decreto del Presidente del Consiglio dei ministri 13 giugno 2008, recante delega di funzioni del Presidente del Consiglio dei Ministri in materia pubblica amministrazione ed innovazione al Ministro senza portafoglio on. prof. Renato Brunetta;

Acquisito il parere tecnico del Centro nazionale per l'informatica nella pubblica amministrazione di cui al decreto legislativo 12 febbraio 1993, n. 39 e successive modificazioni;

Sentito il Garante per la protezione dei dati personali;

Sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 nella seduta del 13 novembre 2008;

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, 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 nell'art. 1 del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni. Si intende, inoltre, per:
a) codice: il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82;
b) chiavi: la coppia di chiavi asimmetriche come definite all'articolo 1, comma 1, lettere h) e i), del codice;
c) CNIPA: il centro nazionale per l'informatica nella pubblica amministrazione;
d) compromissione della chiave privata: la sopravvenuta assenza di affidabilità nelle caratteristiche di sicurezza della chiave crittografica privata;
e) dati per la creazione della firma: l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica;
f) evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
g) funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;
h) 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;
i) marca temporale: il riferimento temporale che consente la validazione temporale;
l) registro dei certificati: la combinazione di uno o più archivi informatici, tenuto dal certificatore, contenente tutti i certificati emessi;
m) riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.

Art. 2. Ambito di applicazione

1. Il presente decreto stabilisce, ai sensi degli articoli 20, 24, comma 4, 27, 28, 29, 30 e 32 del codice, le regole tecniche per la generazione, apposizione e verifica delle firme elettroniche qualificate e per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati.

2. Le disposizioni di cui al titolo II si applicano ai certificatori che rilasciano al pubblico certificati qualificati in conformità al codice.

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

4. I certificatori accreditati rendono disponibile ai propri titolari 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 del Parlamento europeo e del Consiglio, pubblicata nella Gazzetta Ufficiale dell'Unione europea, Serie L, n. 13 del 19 gennaio 2000, è consentito di circolare liberamente nel mercato interno.

Titolo II

REGOLE TECNICHE DI BASE

Art. 3. Norme tecniche di riferimento

1. I dispositivi sicuri per la generazione delle firme di cui all'art. 35 del codice sono conformi alle norme generalmente riconosciute a livello internazionale.

2. Gli algoritmi di generazione e verifica delle firme, le caratteristiche delle chiavi utilizzate, le funzioni di hash, i formati e le caratteristiche dei certificati qualificati, le caratteristiche delle firme digitali e delle marche temporali, il formato dell'elenco di cui all'art. 39 del presente decreto, sono definiti, anche ai fini del riconoscimento e della verifica del documento informatico, con deliberazioni del CNIPA e pubblicati sul sito internet dello stesso Centro nazionale.

3. Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, non produce gli effetti di cui all'art. 21, comma 2, del codice, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità 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 può essere attribuita ad un solo titolare.

2. Se il soggetto appone la sua firma per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del codice, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.

3. Se la procedura automatica fa uso di un insieme di dispositivi sicuri per la generazione delle firme del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

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 informazioni sullo stato di validità del certificato 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 comma 4, salvo che, con riferimento esclusivo alle chiavi di cui al medesimo comma 4, lettera b), il CNIPA non ne autorizzi l'utilizzo per altri scopi.

6. Le caratteristiche quantitative e qualitative delle chiavi sono tali da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche, in conformità con quanto indicato dal CNIPA nella deliberazione di cui all'art. 3, comma 2.

Art. 5. Generazione delle chiavi

1. La generazione della coppia di chiavi è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e un adeguato livello di sicurezza della coppia generata, nonché la segretezza della chiave privata.

2. Il sistema di generazione della coppia di chiavi comunque assicura:
a) la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
b) l'utilizzo di algoritmi che consentano l'equiprobabilità di generazione di tutte le coppie possibili;
c) l'autenticazione informatica del soggetto che attiva la procedura di generazione.

Art. 6. Modalità di generazione delle chiavi

1. Le chiavi di certificazione possono essere generate esclusivamente in presenza del 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, avviene all'interno del dispositivo sicuro per la generazione delle firme, che è rilasciato o indicato dal certificatore.

4. Il certificatore è tenuto ad 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. 35 del codice e all'art. 9 del presente decreto.

5. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo sicuro per la generazione delle firme fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art. 7. Conservazione delle chiavi e dei dati per la creazione della firma

1. E' 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 e di riservatezza delle chiavi stesse.

3. Il titolare della coppia di chiavi:
a) assicura la custodia del dispositivo di firma in conformità all'art. 32, comma 1, del codice, in ottemperanza alle indicazioni fornite dal certificatore;
b) conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
c) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso, o qualora abbia il ragionevole dubbio che essi siano stati usati abusivamente da persone non autorizzate;
d) mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma.

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 assicura:
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 è isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto.

3. L'accesso al sistema è controllato e ciascun utente preventivamente identificato per l'accesso fisico e autenticato per l'accesso logico. Ogni sessione di lavoro è registrata nel giornale di controllo.

4. Il sistema è dotato di strumenti di controllo della propria configurazione che consentano di verificare l'autenticità e l'integrità del software installato e l'assenza di programmi non previsti dalla procedura e di dati residuali provenienti dalla generazione di coppie di chiavi precedenti che possano inficiare l'equiprobabilità della generazione di quelle successive.

Art. 9. Dispositivi sicuri e procedure per la generazione della firma

1. In aggiunta a quanto previsto all'art. 35 del codice, la generazione della firma avviene all'interno di un dispositivo sicuro per la generazione delle firme, così che non sia possibile l'intercettazione della chiave privata utilizzata.

2. Il dispositivo sicuro per la generazione delle firme deve poter essere attivato esclusivamente dal titolare mediante codici personali prima di procedere alla generazione della firma.

3. Il CNIPA, nell'ambito dell'attività di cui agli articoli 29 e 31 del codice, valuta l'adeguatezza tecnologica della modalità di gestione dei codici personali anche in relazione al dispositivo di firma utilizzato.

4. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma prevista dall'art. 35 del codice è effettuata secondo criteri non inferiori a quelli previsti:
a) dal livello EAL 4+ in conformità ai Profili di Protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni;
b) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai Profili di Protezione o traguardi di sicurezza giudicati adeguati ai sensi dell'art. 35, commi 5 e 6 del codice, e successive modificazioni.

5. La certificazione di sicurezza di cui al comma 4 può inoltre essere effettuata secondo i criteri previsti dal livello di valutazione E3 e robustezza HIGH dell'ITSEC, o superiori, con un traguardo di sicurezza giudicato adeguato dal CNIPA nell'ambito dell'attività di cui agli articoli 29 e 31 del codice.

6. La personalizzazione del dispositivo sicuro di firma garantisce almeno:
a) l'acquisizione da parte del certificatore dei dati identificativi del dispositivo sicuro per la generazione delle firme utilizzato e la loro associazione al titolare;
b) la registrazione nel dispositivo sicuro per la generazione delle firme del certificato qualificato, relativo alle chiavi di sottoscrizione del titolare.

7. La personalizzazione del dispositivo sicuro per la generazione delle firme può prevedere, per l'utilizzo nelle procedure di firma, la registrazione, nel dispositivo sicuro per la generazione delle firme, 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.

8. La personalizzazione del dispositivo sicuro per la generazione delle firme è registrata nel giornale di controllo.

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

10. I certificatori che rilasciano certificati qualificati forniscono almeno un sistema che consenta la generazione delle firme digitali.

Art. 10. Verifica delle firme digitali

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

2. Il sistema di verifica delle firme digitali:
a) presenta almeno sinteticamente lo stato di aggiornamento delle informazioni di validità dei certificati di certificazione presenti nell'elenco pubblico;
b) visualizza le informazioni presenti nel certificato qualificato, in attuazione di quanto stabilito nell'art. 28, comma 3, del codice, nonché le estensioni obbligatorie nel certificato qualificato (qcStatements), indicate nel provvedimento di cui all'art. 3, comma 2;
c) consente l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori.

3. Il CNIPA, ai sensi dell'art. 31 del codice, accerta la conformità dei sistemi di verifica di cui al comma 1 alle norme del codice e alle presenti regole tecniche.

Art. 11. Informazioni riguardanti i certificatori

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi del codice forniscono al CNIPA le seguenti informazioni e documenti a loro relativi:
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 di cui al successivo art. 31;
g) manuale operativo di cui al successivo art. 36;
h) relazione sulla struttura organizzativa;
i) copia di una polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi.

2. Il CNIPA rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), d), e), g) al fine di rendere pubbliche le informazioni che individuano il certificatore qualificato. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.

Art. 12. Comunicazione tra certificatore e CNIPA

1. I certificatori che rilasciano al pubblico certificati qualificati comunicano al CNIPA la casella di posta elettronica certificata da utilizzare per realizzare un sistema di comunicazione attraverso il quale scambiare le informazioni previste dal presente decreto.

2. Il CNIPA rende disponibile sul proprio sito internet l'indirizzo della propria casella di posta elettronica certificata.

Art. 13. Generazione delle chiavi di certificazione

1. La generazione delle chiavi di certificazione avviene in modo conforme a quanto previsto dalle presenti regole tecniche.

2. Per ciascuna chiave di certificazione il certificatore genera 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 sono 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. 32 del codice, emettendo il certificato qualificato il certificatore:
a) si accerta dell'autenticità della richiesta;
b) nel caso di chiavi generate dal certificatore, assicura la consegna al legittimo titolare ovvero, nel caso di chiavi non generate dal certificatore, verifica il possesso della chiave privata da parte del titolare e il corretto funzionamento della coppia di chiavi.

2. Il certificato qualificato è generato con un sistema conforme a quanto previsto dall'art. 29.

3. Il termine del periodo di validità del certificato qualificato è anteriore al termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità.

4. L'emissione dei certificati qualificati è registrata nel giornale di controllo specificando il riferimento temporale relativo alla registrazione.

Art. 15. Informazioni contenute nei certificati qualificati

1. Fatto salvo quanto previsto dall'art. 28 del codice, i certificati qualificati contengono almeno le seguenti ulteriori 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 ai sensi di quanto previsto nell'art. 28 del codice sono utilizzabili unicamente per identificare il titolare della firma digitale, per verificare la firma del documento informatico, nonché per indicare eventuali qualifiche specifiche del titolare.

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

4. Le informazioni e le qualifiche di cui all'art. 28, comma 3, lettera a) del Codice, codificate secondo le modalità indicate dalla delibera del CNIPA prevista ai sensi dell'art. 38, comma 4, del presente decreto, sono inserite d'ufficio dal certificatore nel certificato qualificato, nel caso in cui l'organizzazione di appartenenza abbia autorizzato la richiesta di emissione del certificato medesimo. In quest'ultimo caso l'organizzazione richiedente assume l'impegno di richiedere la revoca del certificato qualificato qualora venga a conoscenza della variazione delle informazioni contenute nello stesso.

5. Il certificatore determina il periodo di validità dei certificati qualificati anche in funzione della robustezza crittografica delle chiavi impiegate.

6. Il CNIPA, ai sensi dell'art. 3, comma 2, determina il periodo massimo di validità del certificato qualificato in funzione degli algoritmi e delle caratteristiche delle chiavi.

7. Il certificatore custodisce le informazioni di cui all'art. 32, comma 3, lettera j) del codice, per un periodo pari a 20 (venti) anni dalla data di emissione del certificato qualificato, salvo quanto previsto dall'art. 11 del decreto legislativo n. 196 del 2003.

Art. 16. Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'articolo 36 del codice, il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme.

2. Il certificatore conserva le richieste di revoca e sospensione per lo stesso periodo previsto all'art. 15, comma 7.

Art. 17. Codice di emergenza

1. Per ciascun certificato qualificato emesso il certificatore fornisce al titolare almeno un codice riservato, da utilizzare per richiedere la sospensione del certificato nei casi di emergenza indicati nel manuale operativo e comunicati al titolare.

2. La richiesta di cui al comma 1 è 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.

Art. 18. 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 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.

4. Il certificatore comunica tempestivamente l'avvenuta revoca al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta revocato.

Art. 19. Revoca su iniziativa del certificatore

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

Art. 20. Revoca su richiesta del titolare

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

2. Le modalità di inoltro della richiesta sono indicate dal certificatore nel manuale operativo di cui al successivo art. 36.

3. Il certificatore verifica l'autenticità della richiesta e procede alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal precedente comma 2.

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

Art. 21. Revoca su richiesta del terzo interessato

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

2. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca di cui al comma 1 è inoltrata non appena il terzo venga a conoscenza della variazione di stato.

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

Art. 22. Sospensione dei certificati qualificati

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

2. Il certificatore comunica tempestivamente l'avvenuta sospensione al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.

3. Il certificatore indica nel manuale operativo, ai sensi dell'art. 36, comma 3, lettera l), la durata massima del periodo di sospensione e le azioni intraprese al termine dello stesso in assenza di diverse indicazioni da parte del soggetto che ha richiesto la sospensione.

4. In caso di revoca di un certificato qualificato sospeso, la data della stessa decorre dalla data di inizio del periodo di sospensione.

5. La sospensione e la cessazione della stessa sono annotate nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

6. La cessazione dello stato di sospensione del certificato, che sarà considerato come mai sospeso, è tempestivamente comunicata al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato ha cambiato stato.

Art. 23. Sospensione su iniziativa del certificatore

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

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

Art. 24. Sospensione su richiesta del titolare

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

2. Il certificatore verifica l'autenticità della richiesta e procede alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal precedente comma 1.

Art. 25. Sospensione su richiesta del terzo interessato

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

Art. 26. Sostituzione delle chiavi di certificazione

1. La procedura di sostituzione delle chiavi, generate dal certificatore in conformità all'art. 13 del presente decreto, assicura che non siano stati emessi certificati qualificati con data di scadenza posteriore al periodo di validità del certificato relativo alla coppia sostituita.

2. I certificati generati a seguito della sostituzione delle chiavi di certificazione sono inviati al CNIPA.

Art. 27. 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;
b) malfunzionamento del dispositivo sicuro per la generazione delle firme;
c) cessazione dell'attività.

2. La revoca è comunicata entro ventiquattro ore al CNIPA e resa nota a tutti i titolari di certificati qualificati sottoscritti con la chiave privata la cui corrispondente chiave pubblica è contenuta nel certificato revocato.

3. La revoca di certificati di cui al comma 1, pubblicati dal CNIPA nell'elenco pubblico dei certificatori di cui all'art. 39, è resa nota attraverso il medesimo elenco.

Art. 28. Requisiti di sicurezza dei sistemi operativi

1. I sistemi operativi 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 stati oggetto di opportune personalizzazioni atte a innalzarne il livello di sicurezza (hardening).

2. Ai sensi dell'art. 31 del codice, il CNIPA verifica l'idoneità delle personalizzazioni di cui al comma 1 e indica al certificatore eventuali azioni correttive.

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

Art. 29. Sistema di generazione dei certificati qualificati

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

2. L'entrata e l'uscita dai locali protetti è registrata sul giornale di controllo.

3. L'accesso ai sistemi di elaborazione è 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 sono registrati sul giornale di controllo.

Art. 30. Accesso del pubblico ai certificati

1. Le liste dei certificati revocati e sospesi sono rese pubbliche.

2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico nonché comunicati a terzi, al fine di verificare le firme digitali, 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.

Art. 31. Piano per la sicurezza

1. Il certificatore definisce un piano per la sicurezza nel quale sono contenuti almeno i seguenti elementi:
a) struttura generale, modalità operativa e struttura logistica;
b) descrizione dell'infrastruttura di sicurezza fisica rilevante ai fini dell'attività di certificatore;
c) allocazione dei servizi e degli uffici negli immobili rilevanti ai fini dell'attività di certificatore;
d) descrizione delle funzioni del personale e sua allocazione ai fini dell'attività di certificatore;
e) attribuzione delle responsabilità;
f) algoritmi crittografici o altri sistemi utilizzati;
g) descrizione delle procedure utilizzate nell'attività di certificatore;
h) descrizione dei dispositivi installati;
i) descrizione dei flussi di dati;
l) procedura di gestione delle copie di sicurezza dei dati;
m) procedura di continuità operativa del servizio di pubblicazione delle liste di revoca e sospensione;
n) analisi dei rischi;
o) descrizione delle contromisure;
p) descrizione delle verifiche e delle ispezioni;
q) descrizione delle misure adottate ai sensi degli articoli 28, comma 1 e 43, comma 2;
r) procedura di gestione dei disastri.

2. Il piano per la sicurezza, sottoscritto dal legale rappresentante del certificatore, è consegnato al CNIPA in busta sigillata o inviato, cifrato ai fini di riservatezza, in base alle indicazioni fornite dal CNIPA.

3. Il piano per la sicurezza si attiene almeno 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. 32. Giornale di controllo

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate anche 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 è apposto un riferimento temporale.

4. Il giornale di controllo è 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 è verificata con frequenza almeno mensile.

6. Le registrazioni contenute nel giornale di controllo sono conservate per un periodo pari a venti anni, salvo quanto previsto dall'art. 11 del decreto legislativo n. 196 del 2003.

Art. 33. Sistema di qualità del certificatore

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

2. Il manuale della qualità è depositato presso il CNIPA e reso disponibile presso il certificatore.

Art. 34. Organizzazione del personale addetto al servizio di certificazione

1. Fatto salvo quanto previsto al comma 3, l'organizzazione del certificatore prevede almeno le seguenti figure professionali:
a) responsabile della sicurezza;
b) responsabile del servizio di certificazione e validazione temporale;
c) responsabile della conduzione tecnica dei sistemi;
d) responsabile dei servizi tecnici e logistici;
e) responsabile delle verifiche e delle ispezioni (auditing).

2. Non è possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1.

3. Ferma restando la responsabilità del certificatore, l'organizzazione dello stesso può prevedere che alcune delle suddette responsabilità siano affidate ad altre organizzazioni. In questo caso il responsabile della sicurezza o altro dipendente appositamente designato gestisce i rapporti con tali figure professionali.

4. In nessun caso quanto previsto al comma 3 si applica per le figure professionali di cui al comma 1, lettere a) ed e).

Art. 35. Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'art. 34 del presente decreto deve aver maturato una esperienza professionale nelle tecnologie informatiche e delle telecomunicazioni almeno quinquennale.

2. Per ogni aggiornamento apportato al sistema di certificazione è previsto un apposito addestramento.

Art. 36. 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 è depositato presso il CNIPA e pubblicato a cura del certificatore in modo da essere consultabile per via telematica.

3. Il manuale contiene 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 di inoltro delle richieste e della gestione di sospensione e revoca dei certificati;
m) modalità di sostituzione delle chiavi;
n) modalità di gestione del registro dei certificati;
o) modalità di accesso al registro dei certificati;
p) modalità per l'apposizione e la definizione del riferimento temporale;
q) modalità di protezione dei dati personali;
r) modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 10, comma 1 del presente decreto;
s) modalità operative per la generazione della firma digitale.

Art. 37. Riferimenti temporali opponibili ai terzi

1. I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del codice.

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. 20, comma 3 del codice.

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. Costituiscono inoltre 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, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del codice;
d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14 , comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il decreto del Presidente della Repubblica 12 gennaio 2007, n. 18.

Titolo III

CERTIFICATORI ACCREDITATI

Art. 38. Obblighi per i certificatori accreditati

1. Il certificatore accreditato genera un certificato qualificato per ciascuna delle chiavi di firma elettronica o qualificata utilizzate dal CNIPA per la sottoscrizione dell'elenco pubblico dei certificatori, lo pubblica nel proprio registro dei certificati e lo rende accessibile per via telematica al fine di verificare la validità delle chiavi utilizzate dal CNIPA. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.

2. Il certificatore accreditato garantisce l'interoperabilità del prodotto di verifica di cui all'art. 10 del presente decreto con i documenti informatici sottoscritti mediante firma digitale ad opera del CNIPA, nell'ambito delle attività di cui all'art. 31 del codice.

3. Il certificatore accreditato mantiene copia della lista, sottoscritta dal CNIPA, dei certificati relativi alle chiavi di certificazione di cui all'art. 39, comma 1, lettera e) del presente decreto, che rende accessibile per via telematica per la specifica finalità della verifica delle firme digitali.

4. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 29, comma 1 del codice, svolgono la propria attività in conformità con quanto previsto dalla deliberazione CNIPA, 17 febbraio 2005, n. 4, recante regole per il riconoscimento e la verifica del documento informatico e successive modificazioni.

5. I prodotti di generazione e verifica delle firme digitali forniti dal certificatore accreditato ai sensi degli articoli 9, comma 10 e 10, comma 1, non devono consentire a quest'ultimo di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.

Art. 39. Elenco pubblico dei certificatori accreditati

1. L'elenco pubblico dei certificatori accreditati tenuto dal CNIPA ai sensi dell'art. 29, comma 6, del codice, contiene per ogni certificatore accreditato almeno le seguenti informazioni:
a) denominazione;
b) sede legale;
c) rappresentante legale;
d) indirizzo internet;
e) lista dei certificati delle chiavi di certificazione;
f) manuale operativo;
g) data di accreditamento volontario;
h) eventuale data di cessazione.

2. L'elenco pubblico è sottoscritto e reso disponibile per via telematica dal CNIPA al fine di verificare le firme digitali e diffondere i dati dei certificatori accreditati. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge. Il CNIPA stabilisce il formato dell'elenco pubblico attraverso propria deliberazione.

3. L'elenco pubblico è sottoscritto dal Presidente del CNIPA o dai soggetti da lui designati, mediante firma elettronica o qualificata.

4. Nella Gazzetta Ufficiale della Repubblica italiana è dato avviso:
a) dell'indicazione dei soggetti preposti alla sottoscrizione dell'elenco pubblico di cui al comma 3;
b) del valore dei codici identificativi del certificato relativo alle chiavi utilizzate per la sottoscrizione dell'elenco pubblico, generati attraverso gli algoritmi di cui all'art. 3 del presente decreto;
c) con almeno sessanta giorni di preavviso rispetto alla scadenza del certificato, della sostituzione delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico;
d) della revoca dei certificati utilizzati per la sottoscrizione dell'elenco pubblico sopravvenuta per ragioni di sicurezza.

Art. 40. Rappresentazione del documento informatico

1. Il certificatore indica nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per evitare le conseguenze previste dall'art. 3, comma 3.

Art. 41. 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.

2. La modalità di rappresentazione dei limiti d'uso e di valore di cui all'articolo 28, comma 3, del codice è definita dal CNIPA con il provvedimento di cui all'art. 3, comma 2 del presente decreto.

Art. 42. Verifica delle marche temporali

1. I certificatori accreditati forniscono ovvero indicano almeno un sistema, conforme al successivo comma 2, che consenta di effettuare la verifica delle marche temporali.

2. Il CNIPA con il provvedimento di cui all'art. 3, comma 2, del presente decreto stabilisce le regole di interoperabilità per la verifica della marca temporale, anche associata al documento informatico cui si riferisce.

Titolo IV

REGOLE PER LA VALIDAZIONE TEMPORALEMEDIANTE MARCA TEMPORALE

Art. 43. Validazione temporale con marca temporale

1. Una evidenza informatica è sottoposta a validazione temporale mediante generazione e applicazione di una marca temporale alla relativa impronta.

2. Le marche temporali sono generate da un apposito sistema di validazione temporale, sottoposto ad opportune personalizzazioni atte a innalzarne il livello di sicurezza, in grado di:
a) garantire l'esattezza del riferimento temporale conformemente a quanto richiesto dal presente decreto;
b) generare la struttura dei dati temporali secondo quanto specificato negli articoli 44 e 47 del presente decreto;
c) sottoscrivere digitalmente la struttura di dati di cui alla lettera b).

3. L'evidenza informatica da sottoporre a validazione temporale può essere costituita da un insieme di impronte.

Art. 44. Informazioni contenute nella marca temporale

1. Una marca temporale contiene 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 temporale;
e) riferimento temporale della generazione della marca temporale;
f) identificativo della funzione di hash utilizzata 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 codice identificativo dell'oggetto a cui appartiene l'impronta di cui al comma 1, lettera g).

Art. 45. Chiavi di marcatura temporale

1. Dal certificato relativo alla coppia di chiavi utilizzate per la validazione temporale deve essere possibile individuare il sistema di validazione temporale.

2. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite ed un nuovo certificato è emesso, in relazione alla robustezza delle chiavi crittografiche utilizzate, dopo non più di tre mesi di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato. Detto periodo è indicato nel manuale operativo e ritenuto congruente alla presente disposizione dal CNIPA.

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

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

Art. 46. Gestione dei certificati e delle chiavi

1. Alle chiavi di certificazione utilizzate, ai sensi dell'art. 45, comma 3 del presente decreto, 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 a quanto stabilito ai sensi dell'art. 3, comma 2, contengono l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 47. Precisione dei sistemi di validazione temporale

1. Il riferimento temporale assegnato ad una marca temporale coincide con il momento della sua generazione, 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.

2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC).

Art. 48. Sicurezza dei sistemi di validazione temporale

1. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento del sistema di validazione temporale in modo da renderlo incompatibile con i requisiti previsti dal presente decreto, ed in particolare con quello di cui all'art. 47, comma 1, è annotato sul giornale di controllo e causa il blocco del sistema medesimo.

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

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

4. Ai sensi dell'art. 31 del codice, il CNIPA verifica le equivalenze dichiarate dal certificatore ai sensi del precedente comma 3.

Art. 49. 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 venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.

2. La marca temporale è valida per il periodo di conservazione stabilito o concordato con il certificatore di cui al comma 1.

Art. 50. Richiesta di marca temporale

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

2. La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale.

3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'articolo 3 del presente decreto.

4. La generazione delle marche temporali garantisce 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.

Titolo V

DISPOSIZIONI FINALI

Art. 51. Valore della firma digitale nel tempo

1. La firma digitale, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma digitale in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.

Art. 52. Cessazione dell'attività di certificatore

1. Qualora il certificatore qualificato cessi la propria attività senza indicare un certificatore sostitutivo ai sensi dell'art. 37, comma 2, del codice e senza garantire la conservazione e la disponibilità della documentazione prevista dal codice e dal presente decreto, il CNIPA, nell'ambito dei poteri di vigilanza e controllo previsti dall'articolo 31 del codice, si rende depositario di quest'ultima.

Art. 53. Disposizioni finali

1. Il presente decreto entra in vigore decorsi centottanta giorni dalla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

2. Dall'entrata in vigore del presente decreto è abrogato il decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, 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 27 aprile 2004, n. 98.

Il presente decreto sarà inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.