

D.P.C.M. 8 febbraio 1999

"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513."

II PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;

Visto l'articolo 3 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;

Sentita l'Autorità per l'informatica nella pubblica amministrazione;

Visto il decreto del Presidente del Consiglio dei Ministri del 30 ottobre 1998, con il quale sono state conferite al Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, sen. prof. Franco Bassanini, le funzioni di coordinamento delle attività, anche di carattere normativo, inerenti all'attuazione delle leggi 15 marzo 1997, n. 59, 15 maggio 1997, n. 127 e 16 giugno 1998, n. 191, nonché i compiti inerenti alla disciplina dei sistemi informatici presso le pubbliche amministrazioni;

DECRETA:

Art. 1

1. Il presente decreto stabilisce le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, di cui all'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513 e detta altresì le misure tecniche, organizzative e gestionali di cui all'art. 3, comma 3, dello stesso decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Art. 2

1. Le regole tecniche, di cui all'art. 1, sono riportate nell'allegato tecnico del presente decreto, suddivise in cinque titoli recanti: Regole tecniche di base, regole tecniche per la certificazione delle chiavi, regole tecniche sulla validazione temporale e per la protezione dei documenti informatici, regole tecniche per le pubbliche amministrazioni e disposizioni finali.

Art. 3

1. Le firme digitali certificate ai sensi dell'art. 8, comma 4, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, sono considerate equivalenti a quelle generate in conformità con le regole tecniche stabilite dal presente decreto.
2. I prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione Europea o dello Spazio economico europeo in conformità dei regolamenti vigenti, sono ritenuti conformi alle regole tecniche stabilite dal presente decreto se tali regolamenti assicurano livelli equivalenti di funzionalità e sicurezza.
3. I commi 1 e 2 del presente articolo si applicano anche agli Stati non appartenenti all'Unione Europea con i quali siano stati stipulati specifici accordi di riconoscimento reciproco.

Roma, 8 febbraio 1999
p. il Presidente: Bassanini

ALLEGATO TECNICO

TITOLO I REGOLE TECNICHE DI BASE

Art. 1 Definizioni

1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute nell'art. 1 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513. S'intende, inoltre:
 - . per "titolare" di una coppia di chiavi asimmetriche, il soggetto a cui è attribuita la firma digitale generata con la chiave privata della coppia, ovvero il responsabile del servizio o della funzione che utilizza la firma mediante dispositivi automatici;
 - b. per "impronta" di una sequenza di simboli binari, la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;
 - c. per "funzione di hash", una funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.
 - d. per "dispositivo di firma", un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali;
 - e. per "evidenza informatica", una sequenza di simboli binari che può essere elaborata da una procedura informatica;
 - f. per "marca temporale", un'evidenza informatica che consente la validazione temporale;

Art. 2 Algoritmi di generazione e verifica delle firme digitali

1. Per la generazione e la verifica delle firme digitali possono essere utilizzati i seguenti algoritmi:
 - . RSA (Rivest-Shamir-Adleman algorithm).
 - b. DSA (Digital Signature Algorithm).

Art. 3 Algoritmi di hash

1. La generazione dell'impronta si effettua impiegando una delle seguenti funzioni di hash, definite nella norma ISO/IEC 10118-3:1998:
 - . Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160;
 - b. Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

Art. 4 Caratteristiche generali delle chiavi

1. Una coppia di chiavi può essere attribuita ad un solo titolare.
2. Se la firma del titolare viene apposta per mezzo di una procedura automatica, deve essere utilizzata una chiave diversa da tutte le altre in possesso del sottoscrittore.

3. Se la procedura automatica fa uso di più dispositivi per apporre la firma del medesimo titolare, deve essere utilizzata una chiave diversa per ciascun dispositivo.
4. Ai fini del presente decreto, le chiavi 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 ai certificati ed alle loro liste di revoca (CRL) o sospensione (CSL);
 - c. chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.
5. Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia.
6. La lunghezza minima delle chiavi è stabilita in 1024 bit.
7. Il soggetto certificatore determina il termine di scadenza del certificato ed il periodo di validità delle chiavi in funzione degli algoritmi impiegati, della lunghezza delle chiavi e dei servizi cui esse sono destinate.

Art. 5

Generazione delle chiavi

1. La generazione della coppia di chiavi deve essere effettuata mediante apparati e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.
2. Il sistema di generazione delle chiavi deve comunque assicurare:
 - a. la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
 - b. l'equiprobabilità di generazione di tutte le coppie possibili;
 - c. l'identificazione del soggetto che attiva la procedura di generazione.
3. La rispondenza dei dispositivi di generazione delle chiavi ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC o superiori.

Art. 6

Modalità di generazione delle chiavi

1. La generazione delle chiavi di certificazione e marcatura temporale può essere effettuata esclusivamente dal responsabile del servizio che utilizzerà le chiavi.
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 di firma.

Art. 7

Generazione delle chiavi al di fuori del dispositivo di firma

1. Se la generazione delle chiavi avviene su un sistema diverso da quello destinato all'uso della chiave privata, il sistema di generazione deve assicurare:
 - a. l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura;
 - b. il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui

verrà utilizzata.

2. Il sistema di generazione deve essere isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto contro i rischi di interferenze ed intercettazioni.
3. L'accesso al sistema deve essere controllato e ciascun utente preventivamente identificato. Ogni sessione di lavoro deve essere registrata nel giornale di controllo.
4. Prima della generazione di una nuova coppia di chiavi, l'intero sistema deve procedere alla verifica della propria configurazione, dell'autenticità ed integrità del software installato e dell'assenza di programmi non previsti dalla procedura.
5. La conformità del sistema ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC, o superiori.

Art. 8

Conservazione delle chiavi

1. Le chiavi private sono conservate e custodite all'interno di un dispositivo di firma. È possibile utilizzare lo stesso dispositivo per conservare più chiavi.
2. È vietata la duplicazione della chiave privata o dei dispositivi che la contengono.
3. Per fini particolari di sicurezza, è consentita la suddivisione della chiave privata su più dispositivi di firma.
4. Il titolare delle chiavi deve:
 - a. conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
 - b. conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
 - c. richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi.

Art. 9

Formato della firma

1. Le firme generate secondo le regole contenute nel presente decreto debbono essere conformi a norme emanate da enti riconosciuti a livello nazionale od internazionale ovvero a specifiche pubbliche (Publicly Available Specification - PAS).
2. Alla firma digitale deve essere allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Art. 10

Generazione e verifica delle firme

1. Gli strumenti e le procedure utilizzate per la generazione, l'apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, chiaramente e senza ambiguità, i dati a cui la firma si riferisce e richiedere conferma della volontà di generare la firma.
2. Il comma 1 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del sottoscrittore.
3. La generazione della firma deve avvenire all'interno di un dispositivo di firma così che non sia possibile

l'intercettazione del valore della chiave privata utilizzata.

4. Prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all'identificazione del titolare.
5. La conformità degli strumenti utilizzati per la generazione delle firme ai requisiti di sicurezza imposti dal presente decreto deve essere verificata secondo i criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC o superiori.
6. La conformità degli strumenti utilizzati per la verifica delle firme ai requisiti di sicurezza imposti dal presente decreto deve essere verificata secondo i criteri previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC o superiori.

Art. 11

Informazioni contenute nei certificati

1. I certificati debbono contenere almeno le seguenti informazioni:
 - a. numero di serie del certificato;
 - b. ragione o denominazione sociale del certificatore;
 - c. codice identificativo del titolare presso il certificatore;
 - d. nome cognome e data di nascita ovvero ragione o denominazione sociale del titolare;
 - e. valore della chiave pubblica;
 - f. algoritmi di generazione e verifica utilizzabili;
 - g. inizio e fine del periodo di validità delle chiavi;
 - h. algoritmo di sottoscrizione del certificato.
2. Dal certificato deve potersi desumere in modo inequivocabile la tipologia delle chiavi.
3. Se il certificato è relativo ad una coppia di chiavi di sottoscrizione, in aggiunta alle informazioni prescritte dal comma 1, possono essere indicati:
 - a. eventuali limitazioni nell'uso della coppia di chiavi;
 - b. eventuali poteri di rappresentanza;
 - c. eventuali abilitazioni professionali.
4. Se il certificato è relativo ad una coppia di chiavi di certificazione, in aggiunta alle informazioni prescritte dal comma 1, deve essere altresì indicato l'uso delle chiavi per la certificazione.
5. Se il certificato è relativo ad una coppia di chiavi di marcatura temporale, in aggiunta alle informazioni prescritte dal comma 1, debbono essere indicati:
 - a. uso delle chiavi per la marcatura temporale;
 - b. identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 12

Formato dei certificati

1. I certificati e le relative liste di revoca debbono essere conformi alla norma ISO/IEC 9594-8:1995 con le estensioni definite nella Variante 1, ovvero alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Art. 13

Modalità di accesso al registro dei certificati

1. L'accesso al registro dei certificati mantenuto da ciascun certificatore avviene secondo una modalità compatibile con il protocollo LDAP definito nella specifica pubblica RFC 1777 e successive modificazioni o integrazioni.
2. Il certificatore ha facoltà di fornire modalità di accesso al registro dei certificati aggiuntive rispetto a quella prevista dal comma 1.
3. Ciascun certificatore deve pubblicare gli indirizzi elettronici e telefonici attraverso cui è possibile accedere al registro, attraverso l'elenco pubblico di cui all'articolo 8 comma 3 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

TITOLO II REGOLE TECNICHE PER LA CERTIFICAZIONE DELLE CHIAVI

Art. 14

Chiavi dell'Autorità per l'informatica nella Pubblica Amministrazione

1. L'Autorità per l'informatica nella Pubblica Amministrazione può delegare la certificazione delle proprie chiavi al Centro Tecnico per l'assistenza ai soggetti che utilizzano la rete unitaria della pubblica amministrazione, istituito dall'articolo 17, comma 19, della legge 15 maggio 1997, n. 127.
2. Per ciascuna coppia di chiavi sono pubblicati sulla Gazzetta Ufficiale della Repubblica Italiana uno o più codici identificativi idonei per la verifica del valore della chiave pubblica.

Art. 15

Elenco pubblico dei certificatori

1. L'elenco pubblico tenuto dall'Autorità ai sensi dell'articolo 8, comma 3 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, contiene per ogni certificatore le seguenti informazioni:
 - a. Ragione o denominazione sociale,
 - b. Sede legale,
 - c. Rappresentante legale,
 - d. Nome X.500,
 - e. Indirizzo Internet,
 - f. Elenco numeri telefonici di accesso,
 - g. Lista dei certificati delle chiavi di certificazione,
 - h. Manuale operativo,
 - i. Data di cessazione e certificatore sostitutivo.
2. L'elenco pubblico è sottoscritto dall'Autorità per l'informatica nella Pubblica Amministrazione.

Art. 16

Richiesta di iscrizione all'elenco pubblico dei certificatori

1. Chiunque intenda esercitare l'attività di certificatore deve inoltrare all'Autorità per l'informatica nella Pubblica Amministrazione, secondo le modalità da questa definite con apposita circolare, domanda di

iscrizione nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

2. Alla domanda debbono essere allegati:
 - a. copia del manuale operativo;
 - b. copia del piano per la sicurezza;
 - c. profilo del personale responsabile della generazione delle chiavi, della emissione dei certificati e della gestione del registro delle chiavi;
 - d. copia della polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi.
3. L'Autorità ha facoltà di chiedere integrazioni della documentazione presentata.
4. Entro 60 giorni dalla presentazione la domanda di iscrizione nell'elenco pubblico è accettata ovvero respinta con provvedimento motivato. La richiesta di documentazione integrativa sospende il decorso dei termini.
5. Il Centro Tecnico per l'assistenza ai soggetti che utilizzano la rete unitaria della pubblica amministrazione è iscritto nell'elenco pubblico dei certificatori con riferimento ai compiti definiti dal decreto del Presidente della Repubblica 23 dicembre 1997, n. 522 ed è tenuto all'osservanza delle disposizioni delle presenti regole tecniche.

Art. 17

Iscrizione nell'elenco pubblico dei certificatori

1. Il certificatore, la cui domanda di iscrizione sia stata accettata, deve predisporre con l'Autorità per l'informatica nella Pubblica Amministrazione un sistema di comunicazione sicuro attraverso il quale scambiare le informazioni previste dal presente decreto.
2. Il certificatore deve fornire le informazioni di cui al comma 1 dell'articolo 15, nonché i certificati relativi alle proprie chiavi di certificazione, generati conformemente alle modalità previste dall'articolo 19.
3. Il certificatore deve generare un proprio certificato per ciascuna delle chiavi di firma dell'Autorità per l'informatica nella Pubblica Amministrazione e pubblicarlo nel proprio registro dei certificati.
4. Il certificatore deve mantenere copia della lista, sottoscritta dall'Autorità per l'informatica nella Pubblica Amministrazione, dei certificati relativi alle chiavi di certificazione di cui all'articolo 15, comma 1, lettera g), che deve rendere accessibile per via telematica.

Art. 18

Verifica dei requisiti dei certificatori

1. Al verificarsi di ogni variazione dei requisiti di cui all'art. 16 o, comunque, allo scadere di un anno dalla data della precedente richiesta o comunicazione, il certificatore deve confermare per iscritto all'Autorità per l'informatica nella Pubblica Amministrazione la permanenza dei requisiti per l'esercizio dell'attività di certificazione.
2. Il venir meno di uno o più requisiti tra quelli indicati all'art. 16 è causa di cancellazione dall'elenco.
3. Le modalità di esecuzione delle disposizioni del presente articolo sono stabilite con circolare dell'Autorità per l'informatica nella Pubblica Amministrazione.
4. Per l'esercizio delle attività di verifica e controllo previste dalle presenti disposizioni, l'Autorità per l'informatica nella Pubblica Amministrazione può corrispondere con tutte le amministrazioni e chiedere ad esse notizie ed informazioni utili allo svolgimento dei propri compiti, ai sensi dell'articolo 7, comma 4, del decreto legislativo 12 febbraio 1993, n. 39.

Art. 19

Generazione delle chiavi di certificazione

1. La generazione delle chiavi di certificazione deve avvenire in modo conforme a quanto previsto dagli articoli 5, 6 e 7.
2. Per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

Art. 20

Cessazione dell'attività

1. Il certificatore che intende cessare l'attività è tenuto a comunicare all'Autorità per l'informatica nella Pubblica Amministrazione la data di cessazione con un anticipo di almeno 6 mesi, indicando il certificatore sostitutivo ovvero il depositario del registro dei certificati e della relativa documentazione.
2. L'Autorità per l'informatica nella Pubblica Amministrazione rende nota nell'elenco pubblico la data di cessazione con l'indicazione del certificatore sostitutivo ovvero del depositario del registro dei certificati e della relativa documentazione.
3. Con un anticipo di almeno 6 mesi rispetto alla cessazione dell'attività, il certificatore deve informare i possessori di certificati da esso emessi, specificando che tutti i certificati non scaduti al momento della cessazione debbono essere revocati.

Art. 21

Certificazione tra certificatori

1. È consentito ai certificatori definire accordi di certificazione.
2. Con l'accordo di certificazione, un certificatore emette a favore dell'altro un certificato relativo a ciascuna chiave di certificazione che viene riconosciuta nel proprio ambito.
3. I certificati di cui al comma 2 debbono definire la corrispondenza tra le clausole dei rispettivi manuali operativi considerate equivalenti.

Art. 22

Registrazione dei titolari

1. Per ottenere la certificazione di una chiave pubblica il titolare deve essere preventivamente registrato presso il certificatore. La richiesta di registrazione deve essere redatta per iscritto e deve essere conservata a cura del certificatore per almeno 10 anni.
2. Al momento della registrazione il certificatore deve verificare l'identità del richiedente. È data facoltà al certificatore di definire, pubblicandole nel manuale operativo, le modalità di identificazione degli utenti.
3. Il certificatore deve attribuire a ciascun titolare registrato un codice identificativo di cui garantisce l'univocità nell'ambito dei propri utenti. Al medesimo soggetto sono attribuiti codici identificativi distinti per ciascuno dei ruoli per i quali egli può firmare.

Art. 23

Uso di pseudonimi

1. I dati di cui all'art. 11, comma 1, lettera d) possono essere sostituiti, nel certificato, da uno pseudonimo.

2. La presenza di uno pseudonimo in luogo dei dati anagrafici deve essere esplicitamente indicata nel certificato.
3. Il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno 10 anni dopo la scadenza del certificato.

Art. 24

Obbligo di informazione

1. Il certificatore deve informare espressamente il richiedente la registrazione riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma.
2. Il certificatore deve informare espressamente il titolare in ordine agli accordi di certificazione stipulati con altri certificatori ai sensi dell'articolo 21.

Art. 25

Comunicazione tra certificatore e titolare

1. Al momento della registrazione il certificatore può fornire al titolare gli strumenti necessari per realizzare un sistema di comunicazione sicuro che consenta, quando il titolare non disponga di ulteriori chiavi utilizzabili per la sua autenticazione, di effettuare per via telematica le seguenti operazioni:
 - a. personalizzazione dei dispositivi di firma;
 - b. richiesta della certificazione di chiavi generate al di fuori dell'ambiente del certificatore;
 - c. richiesta di revoca immediata di un certificato.
2. In assenza del sistema di comunicazione sicuro le operazioni di cui al comma 1 debbono essere effettuate presso il certificatore.

Art. 26

Personalizzazione del dispositivo di firma

1. La personalizzazione del dispositivo di firma consiste in:
 - a. acquisizione da parte del certificatore dei dati identificativi del dispositivo di firma utilizzato e loro associazione al titolare;
 - b. registrazione, nel dispositivo di firma, dei dati identificativi del titolare presso il certificatore;
 - c. registrazione, nel dispositivo di firma, dei certificati relativi alle chiavi di certificazione del certificatore.
2. Durante la personalizzazione del dispositivo di firma il certificatore ne verifica il corretto funzionamento.
3. La personalizzazione del dispositivo di firma è registrata nel giornale di controllo.

Art. 27

Richiesta di certificazione

1. Il titolare che intende ottenere la certificazione di una coppia di chiavi deve inoltrare la richiesta, attraverso il sistema di comunicazione di cui all'articolo 25, o con altro meccanismo previsto dal manuale operativo.
2. Nella richiesta debbono essere esplicitamente indicate le informazioni che il soggetto non desidera che siano inserite nel certificato.

3. La richiesta di certificazione deve essere conservata a cura del certificatore per un periodo non inferiore ai 10 anni.

Art. 28

Generazione dei certificati

1. Prima di emettere il certificato il certificatore deve:
 - a. accertarsi dell'autenticità della richiesta;
 - b. verificare che la chiave pubblica di cui si richiede la certificazione non sia stata certificata da uno dei certificatori iscritti nell'elenco.
 - c. richiedere la prova del possesso della chiave privata e verificare il corretto funzionamento della coppia di chiavi, eventualmente richiedendo la sottoscrizione di uno o più documenti di prova.
2. Qualora la verifica di cui alla lettera b) del comma 1 evidenzi la presenza di certificati relativi alla chiave di cui viene richiesta la certificazione rilasciati ad un titolare diverso dal richiedente, la richiesta di certificazione deve essere rigettata. L'evento deve essere registrato nel giornale di controllo e segnalato al titolare della chiave già certificata. Se è stata fornita la prova di possesso di cui al comma 1 lettera c), per la chiave già certificata deve essere avviata la procedura di revoca dei certificati secondo quanto previsto dall'articolo 30.
3. Il certificato deve essere generato con un sistema conforme a quanto previsto dall'articolo 42.
4. Il certificato deve essere pubblicato mediante inserimento nel registro dei certificati gestito dal certificatore. Il momento della pubblicazione deve essere attestato mediante generazione di una marca temporale, che deve essere conservata fino alla scadenza della validità della chiavi.
5. Il certificato emesso e la relativa marca temporale debbono essere inviati al titolare.
6. Per ciascun certificato emesso il certificatore deve fornire al titolare un codice riservato, da utilizzare in caso di emergenza per l'autenticazione della eventuale richiesta di revoca del certificato.
7. La generazione dei certificati è registrata nel giornale di controllo.

Art. 29

Revoca dei certificati relativi a chiavi di sottoscrizione

1. La revoca di un certificato determina la cessazione anticipata della sua validità.
2. La revoca può avvenire su richiesta del titolare o del terzo interessato di cui all'articolo 9, comma 2, lettera c) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, ovvero su iniziativa del certificatore.
3. La revoca del certificato viene effettuata dal certificatore mediante il suo inserimento in una delle liste di certificati revocati (CRL) da lui gestite. La revoca del certificato è efficace a partire dal momento della pubblicazione della lista che lo contiene ed è definitiva.
4. Il momento di pubblicazione della lista deve essere asseverato mediante l'apposizione di una marca temporale.
5. Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il certificatore deve procedere immediatamente alla pubblicazione dell'aggiornamento della lista di revoca.
6. La revoca dei certificati è annotata nel giornale di controllo.

Art. 30

Revoca su iniziativa del certificatore

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

Art. 31

Revoca su richiesta del titolare

1. La richiesta di revoca deve essere redatta per iscritto dal titolare specificando la motivazione della revoca e la sua decorrenza.
2. La richiesta viene di norma inoltrata attraverso il sistema di comunicazione sicuro di cui all'articolo 25.
3. Modalità alternative di inoltro della richiesta debbono essere specificate dal certificatore nel manuale operativo.
4. Il certificatore deve verificare l'autenticità della richiesta e procedere alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con la modalità prevista dal comma 2.
5. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 32

Revoca su richiesta del terzo interessato

1. La richiesta di revoca da parte del terzo interessato di cui all'articolo 9, comma 2, lettera c) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, deve essere inoltrata per iscritto e corredata della documentazione giustificativa.
2. Il certificatore deve notificare la richiesta al titolare.

Art. 33

Sospensione dei certificati

1. La validità di un certificato può essere sospesa su richiesta del titolare o del terzo interessato di cui all'articolo 9, comma 2, lettera c) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, ovvero su iniziativa del certificatore.
2. La sospensione del certificato è effettuata dal certificatore attraverso l'inserimento in una delle liste dei certificati sospesi e diviene efficace dal momento della pubblicazione della lista che lo contiene. La data e l'ora di pubblicazione sono garantite dall'apposizione di una marca temporale.
3. La sospensione dei certificati è annotata nel giornale di controllo.

Art. 34

Sospensione su iniziativa del certificatore

1. Il certificatore che intende sospendere un certificato deve darne preventiva comunicazione al titolare, specificando i motivi della sospensione e la sua durata.
2. L'avvenuta sospensione del certificato deve essere notificata al titolare specificando la data e l'ora a partire dalla quale il certificato risulta sospeso.
3. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave, il certificatore deve procedere immediatamente alla pubblicazione della sospensione.

Art. 35

Sospensione su richiesta del titolare

1. La richiesta di sospensione deve essere redatta per iscritto dal titolare, specificando la motivazione ed il periodo durante il quale la validità del certificato deve essere sospesa.
2. La richiesta viene di norma inoltrata attraverso il sistema di comunicazione sicuro di cui all'articolo 25.
3. Modalità alternative di inoltro della richiesta debbono essere specificate dal certificatore nel manuale operativo.
4. Il certificatore deve verificare l'autenticità della richiesta e procedere alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con la modalità prevista dal comma 2.
5. In caso di emergenza è possibile richiedere la sospensione immediata di un certificato utilizzando il codice previsto dal comma 6 dell'articolo 28. La richiesta deve essere successivamente confermata utilizzando una delle modalità previste dal certificatore.

Art. 36

Sospensione su richiesta del terzo interessato

1. La richiesta di sospensione da parte del terzo interessato di cui all'articolo 9, comma 2, lettera c) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, deve essere inoltrata per iscritto e corredata della documentazione giustificativa.
2. Il certificatore deve notificare la richiesta al titolare.

Art. 37

Sostituzione delle chiavi di certificazione

1. Almeno 90 giorni prima della scadenza del certificato relativo ad una chiave di certificazione il certificatore deve avviare la procedura di sostituzione, generando, con le modalità previste dall'articolo 19, una nuova coppia di chiavi.
2. In aggiunta al certificato previsto dal comma 1, 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 nuova chiave privata.
3. I certificati generati secondo quanto previsto dai commi 1 e 2 debbono essere forniti all'Autorità per l'informatica nella Pubblica Amministrazione, la quale provvede all'aggiornamento della lista di cui all'articolo 15, comma 1, lettera g) ed al suo inoltro ai certificatori per la pubblicazione ai sensi dell'articolo 17, comma 4.

Art. 38

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 segreta;
 - b. guasto del dispositivo di firma;
 - c. cessazione dell'attività.
2. La revoca deve essere notificata entro 24 ore all'Autorità per l'informatica nella Pubblica Amministrazione ed a tutti i possessori di certificati sottoscritti con la chiave segreta appartenente alla coppia revocata.

3. Il certificato revocato deve essere inserito in una lista di revoca aggiornata immediatamente.
4. I certificati per i quali risultino contemporaneamente compromesse sia la chiave di certificazione con cui sono stati sottoscritti, sia quella utilizzata per la generazione della marca temporale di cui al comma 4 dell'articolo 28 debbono essere revocati.
5. L'Autorità per l'informatica nella Pubblica Amministrazione provvede all'aggiornamento della lista di cui all'articolo 15, comma 1, lettera g) ed al suo inoltro ai certificatori per la pubblicazione ai sensi dell'articolo 17, comma 4.

Art. 39

Sostituzione delle chiavi dell'Autorità

1. Almeno 90 giorni prima della scadenza della coppia di chiavi utilizzata per la sottoscrizione dell'elenco pubblico dei certificatori, l'Autorità per l'informatica nella Pubblica Amministrazione provvede alla generazione e certificazione di una nuova coppia di chiavi.
2. Copia degli elementi contenuti nell'elenco pubblico dei certificatori viene sottoscritta con la nuova coppia di chiavi.
3. La lista di cui all'articolo 15, comma 1, lettera g) è inviata ai certificatori per la pubblicazione ai sensi dell'articolo 17, comma 4.

Art. 40

Revoca dei certificati relativi alle chiavi dell'Autorità

1. I certificati relativi alle chiavi dell'Autorità per l'informatica nella Pubblica Amministrazione possono essere revocati solo in caso di compromissione della chiave segreta ovvero di guasto del dispositivo di firma.
2. Nell'ipotesi di cui al comma 1, l'Autorità per l'informatica nella Pubblica Amministrazione richiede a ciascun certificatore la revoca immediata del certificato ad essa rilasciato ai sensi dell'art. 17 .
3. L'Autorità per l'informatica nella Pubblica Amministrazione provvede alla sostituzione della chiave revocata secondo quanto previsto dall'articolo 39.

Art. 41

Requisiti di sicurezza dei sistemi operativi

1. Il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, deve essere conforme almeno alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC.
2. Il requisito di cui al comma 1 non si applica al sistema operativo dei dispositivi di firma.

Art. 42

Caratteristiche del sistema di generazione dei certificati

1. La generazione dei certificati deve avvenire su un sistema utilizzato esclusivamente per tale funzione, 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 sono registrate sul giornale di controllo.

Art. 43

Registro dei certificati

1. Nel registro dei certificati debbono essere presenti i seguenti elementi:
 - a. i certificati emessi dal certificatore;
 - b. la lista dei certificati revocati;
 - c. la lista dei certificati sospesi.
2. Il certificatore può suddividere le liste dei certificati revocati e sospesi in più liste distinte.
3. Il certificatore può replicare il registro dei certificati su più siti, purché sia garantita la consistenza e l'integrità delle copie.
4. Il registro dei certificati è accessibile a qualsiasi soggetto secondo le modalità previste dall'articolo 13.

Art. 44

Requisiti del registro dei certificati

1. Il certificatore deve mantenere una copia di riferimento del registro dei certificati inaccessibile dall'esterno, allocata su un sistema sicuro installato in locali protetti.
2. Il certificatore deve sistematicamente verificare la conformità tra la copia operativa e la copia di riferimento del registro dei certificati, qualsiasi discordanza deve essere immediatamente segnalata ed annotata nel registro operativo.
3. L'effettuazione delle operazioni che modificano il contenuto del registro dei certificati deve essere possibile solo per il personale espressamente autorizzato.
4. Tutte le operazioni che modificano il contenuto del registro debbono essere registrate sul giornale di controllo.
5. La data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile debbono essere annotate sul giornale di controllo.
6. Almeno una copia di sicurezza della copia operativa e di quella di riferimento del registro dei certificati deve essere conservata in armadi di sicurezza distinti, situati in locali diversi.

Art. 45

Manuale operativo

1. Il manuale operativo definisce le procedure applicate dal certificatore nello svolgimento della propria attività.
2. Il manuale operativo deve essere depositato presso l'Autorità per l'informatica nella Pubblica Amministrazione 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 di quanti accedono per la verifica delle firme;
 - e. definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;

- f. tariffe;
- g. modalità di identificazione e registrazione degli utenti;
- h. modalità di generazione delle chiavi;
- i. modalità di emissione dei certificati;
- l. modalità 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 di protezione della riservatezza;
- q. procedure di gestione delle copie di sicurezza;
- r. procedure di gestione degli eventi catastrofici.

Art. 46

Piano per la sicurezza

1. Il responsabile della sicurezza deve definire un piano per la sicurezza nel quale debbono essere contenuti almeno i seguenti elementi:
 - . struttura generale, modalità operativa e struttura logistica dell'organizzazione;
 - b. descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza;
 - c. allocazione dei servizi e degli uffici negli immobili dell'organizzazione;
 - d. elenco del personale e sua allocazione negli uffici;
 - e. attribuzione delle responsabilità;
 - f. algoritmi crittografici utilizzati;
 - g. descrizione delle procedure utilizzate nell'attività 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.
1. Il piano per la sicurezza deve essere conforme a quanto previsto dall'articolo 9, comma 2, lettera f) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, con riguardo alla sicurezza dei dati personali.

Art. 47

Giornale di controllo

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il certificatore, allorché si verificano le condizioni previste dal presente decreto.
2. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.
3. A ciascuna registrazione deve essere associata la data e l'ora in cui essa è stata effettuata.

4. Il giornale di controllo deve essere tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione con la necessaria accuratezza di tutti gli eventi rilevanti ai fini della sicurezza.
5. L'integrità del giornale di controllo deve essere verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo debbono essere archiviate con le modalità previste dal presente decreto e conservate per un periodo non inferiore a 10 anni.

Art. 48

Sistema di qualità del certificatore

1. Entro un anno dall'avvio dell'attività di certificazione, il sistema di qualità del certificatore deve essere certificato secondo le norme ISO 9002.
2. Il manuale della qualità deve essere depositato presso l'Autorità per l'informatica nella Pubblica Amministrazione e disponibile presso il certificatore.

Art. 49

Organizzazione del personale del certificatore

1. L'organizzazione del personale del certificatore 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;
 - i. responsabile dei servizi tecnici;
 - l. responsabile dell'auditing.
1. È possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1 purché tra loro compatibili.
2. Sono compatibili tra loro le funzioni specificate nei sottoindicati raggruppamenti:
 - l. generazione e custodia delle chiavi, generazione dei certificati, personalizzazione dei dispositivi di firma, crittografia, sicurezza dei dati;
 - m. registrazione degli utenti, gestione del registro dei certificati, crittografia, sicurezza dei dati.

Art. 50

Requisiti di onorabilità del certificatore

1. I requisiti di onorabilità richiesti dall'art. 8, comma 3, lettera b) del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, sono quelli stabiliti con il decreto del Ministro del Tesoro, del Bilancio e della Programmazione economica 18 marzo 1998, n. 161.

Art. 51

Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'articolo 49 deve aver maturato una esperienza almeno quinquennale nella analisi, progettazione e conduzione di sistemi informatici.
2. Per ogni aggiornamento apportato al sistema di certificazione deve essere previsto un apposito corso di addestramento.

TITOLO III

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

Art. 52

Validazione temporale

1. Una evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi.
2. Le marche temporali sono generate da un apposito sistema elettronico sicuro in grado di:
 - a. mantenere la data e l'ora conformemente a quanto richiesto dal presente decreto;
 - b. generare la struttura di dati contenente le informazioni specificate dall'articolo 53;
 - c. sottoscrivere digitalmente la struttura di dati di cui alla lettera b).

Art. 53

Informazioni contenute nella marca temporale

1. Una marca temporale deve contenere almeno le seguenti informazioni:
 - a. identificativo dell'emittente;
 - b. numero di serie della marca temporale;
 - c. algoritmo di sottoscrizione della marca temporale;
 - d. identificativo del certificato relativo alla chiave di verifica della marca;
 - e. data ed ora di generazione della marca;
 - f. identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
 - g. valore dell'impronta dell'evidenza informatica.
2. La marca temporale può inoltre contenere un identificatore dell'oggetto a cui appartiene l'impronta di cui alla lettera g) del comma 1.
3. La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato UTC.

Art. 54

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 dopo non più di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.
3. Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale debbono essere utilizzate chiavi di certificazione diverse da quelle utilizzate per i certificati relativi alle normali chiavi di sottoscrizione.

Art. 55

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.

Art. 56

Sicurezza dei sistemi di validazione temporale

1. Ogni sistema di validazione temporale deve produrre un registro operativo su di un supporto non riscrivibile nel quale sono automaticamente registrati gli eventi per i quali tale registrazione è richiesta dal presente decreto.
2. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento dell'apparato in modo da renderlo incompatibile con i requisiti del presente decreto, ed in particolare con quello di cui al comma 1 dell'articolo 55, deve essere annotato sul registro operativo e causare il blocco del sistema.
3. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.
4. La conformità ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo i criteri previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC o superiori. Per le componenti destinate alla sottoscrizione delle marche temporali si applicano in ogni caso le disposizioni dell'articolo 10.

Art. 57

Registrazione delle marche generate

1. Tutte le marche temporali emesse da un sistema di validazione debbono essere conservate in un apposito archivio digitale fino alla scadenza della chiave pubblica della coppia utilizzata per la loro generazione.

Art. 58

Richiesta di validazione temporale

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'inoltro della richiesta di validazione temporale.
2. La richiesta deve contenere l'evidenza informatica alla quale le marche temporali debbono fare riferimento.
3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash previste dal manuale operativo. Debbono essere comunque accettate le funzioni di hash di cui all'articolo 3.
4. La richiesta può specificare l'emissione di più marche temporali per la stessa evidenza informatica. In tal caso debbono essere restituite marche temporali generate con chiavi diverse.
5. La generazione delle marche temporali deve garantire un tempo di risposta, misurato come differenza tra il

momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

Art. 59

Protezione dei documenti informatici

1. Al solo fine di assicurare l'associazione tra documento informatico e le relative marche temporali, il certificatore può conservare, dietro richiesta del soggetto interessato, copia del documento informatico cui la marca temporale si riferisce.
2. Nel manuale operativo debbono essere definite le modalità di conservazione e le procedure per la richiesta del servizio.

Art. 60

Estensione della validità del documento informatico

1. La validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una o più marche temporali.
2. Prima della scadenza della marca temporale, il periodo di validità può essere ulteriormente esteso associando una nuova marca all'evidenza informatica costituita dal documento iniziale, dalla relativa firma e dalle marche temporali già ad esso associate.
3. La presenza di una marca temporale valida associata ad un documento informatico secondo quanto previsto dal comma 2, garantisce la validità del documento anche in caso di compromissione della chiave di sottoscrizione, purché la marca temporale sia stata generata antecedentemente a tale evento.

Art. 61

Archiviazione dei documenti informatici

1. L'archiviazione dei documenti informatici, anche se formati secondo quanto previsto dall'articolo 6, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, può essere effettuata con le modalità previste dalla deliberazione 30 luglio 1998, n. 24 dell'Autorità per l'informatica nella Pubblica Amministrazione e successive modificazioni ed integrazioni.
2. Per i documenti informatici si applicano le procedure previste per i documenti formati all'origine su supporto informatico di cui all'articolo 6, comma 1, lettera b) della deliberazione indicata al comma 1.
3. Ai documenti informatici non si applicano le restrizioni di formato previste dall'articolo 6, comma 1, lettera b) della deliberazione. Il responsabile dell'archiviazione può convertire il documento informatico in uno di tali formati, mantenendo nell'archivio il documento originale come versione iniziale del documento archiviato.

TITOLO IV

REGOLE TECNICHE PER LE PUBBLICHE AMMINISTRAZIONI

Art. 62

Certificazione da parte delle Pubbliche Amministrazioni

1. Secondo quanto previsto dal decreto del Presidente della Repubblica 10 novembre 1997, n. 513, le pubbliche amministrazioni provvedono autonomamente alla certificazione delle chiavi pubbliche dei propri organi e uffici, nell'attività amministrativa di loro competenza, osservando le regole tecniche e di sicurezza previste dagli articoli precedenti. A tal fine possono avvalersi dei servizi offerti da certificatori inclusi nell'elenco pubblico di cui all'articolo 8 dello stesso decreto, nel rispetto delle norme vigenti per l'aggiudicazione dei contratti pubblici.
2. Restano salve le disposizioni del decreto del Presidente della Repubblica 23 dicembre 1997, n. 522, con riferimento ai compiti di certificazione e di validazione temporale del Centro Tecnico per l'assistenza ai soggetti che utilizzano la rete unitaria delle pubbliche amministrazioni, in conformità alle disposizioni dei regolamenti previsti dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.
3. Restano salve le disposizioni contenute nel decreto del Ministero delle finanze 31 luglio 1998, pubblicato nella Gazzetta Ufficiale n. 187 del 12 agosto 1998, concernente le modalità tecniche di trasmissione telematica delle dichiarazioni, e le successive modificazioni ed integrazioni.

TITOLO V DISPOSIZIONI FINALI

Art. 63 Norme transitorie

1. Le disposizioni che richiedono verifiche secondo i criteri previsti da livelli di valutazione ITSEC non si applicano nei diciotto mesi successivi alla data di entrata in vigore delle presenti regole tecniche. Durante il periodo transitorio, il fornitore o il certificatore, secondo le rispettive competenze, devono tuttavia attestare, mediante autodichiarazione, la rispondenza dei dispositivi ai requisiti di sicurezza imposti dalle suddette disposizioni.