CIRCOLARE del 16 febbraio 2001, n. AIPA/CR/27

Art. 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni.

1. Premessa

Com'è noto, l'art. 3 del decreto legislativo 12 febbraio 1993, n. 39, ha introdotto il principio secondo il quale "gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite i sistemi informativi automatizzati".

L'art. 15, comma 2, della legge 15 marzo 1997, n. 59, ha, poi, riconosciuto validità e rilevanza, a tutti gli effetti di legge, agli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici e telematici, demandando a "specifici regolamenti", da emanarsi ai sensi dell'art. 17, comma 2, della legge n. 400/1988, la definizione dei criteri e delle modalità di applicazione della norma.

Con decreto del Presidente della Repubblica 10 novembre 1997, n. 513, è stato emanato il "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici".

I documenti informatici delle pubbliche amministrazioni debbono essere formati e conservati secondo le regole tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione con deliberazione n. 51/2000 del 23 novembre 2000, emanata ai sensi dell'art. 18, comma 3, del citato d.P.R. n. 513/1997.

L'art. 17 del richiamato decreto prevede che le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi di cifratura pubbliche di propria competenza, nel rispetto di quanto prescritto dall'art. 8, in materia di certificazione, sia per le pubbliche amministrazioni che per i privati, e delle regole tecniche di cui all'art. 3.

L'art. 16, comma 1, dell'allegato tecnico al d.P.C.M. 8 febbraio 1999, recante le "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale dei documenti informatici" ai sensi dell'art. 3, comma 1, del d.P.R. n. 513/1997, ha determinato le modalità di presentazione della domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'art.8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513; l'art. 62 dello stesso allegato definisce le regole tecniche per la certificazione da parte delle pubbliche amministrazioni.

Ciò premesso e con riferimento alle norme citate, le pubbliche amministrazioni possono:

a) ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna:

- svolgere in proprio l'attività di certificazione di cui all'art. 8 del decreto 10 novembre 1997, n. 513, ma limitatamente ai propri organi ed uffici ed hanno l'obbligo di iscriversi nell'elenco pubblico dei certificatori, predisposto, tenuto e aggiornato a cura di questa Autorità per l'informatica, secondo le modalità indicate al successivo punto 2, attenendosi alle regole tecniche di cui al d.P.C.M. 8 febbraio 1999;
- rilasciare certificati di firma digitale relativi ai propri organi ed uffici, avvalendosi dei servizi offerti dal Centro tecnico o dai certificatori iscritti nell'elenco di cui sopra, acquisiti nel rispetto della vigente normativa in materia di contratti pubblici; in questo caso non vi è obbligo di iscrizione nel citato elenco pubblico;

b) per la sottoscrizione di documenti informatici di rilevanza interna:

- rilasciare ai propri organi ed uffici firme elettroniche certificate secondo regole tecniche diverse da quelle di cui al d.P.C.M. 8 febbraio 1999;

c) per la formazione e la gestione di documenti informatici per i quali non è prevista la sottoscrizione:

- utilizzare sistemi elettronici di identificazione e autenticazione che l'Amministrazione, nell'ambito della propria autonomia organizzativa, ha ritenuto di adottare.

2. Attività di certificazione ed iscrizione nell'elenco pubblico dei certificatori

Le pubbliche amministrazioni che intendono svolgere l'attività di certificazione di cui all'art. 8 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, nel rispetto di quanto stabilito dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 devono inoltrare all'Autorità per l'informatica nella pubblica amministrazione, domanda di iscrizione nell'elenco pubblico di cui all'art. 8, comma 3, del d.P.R. 10 novembre 1997, n. 513, secondo le modalità che qui di seguito si espongono e che sono disponibili anche sul sito Internet dell'AIPA (www.aipa.it)

2.1 Formalità con le quali deve essere predisposta la domanda e documentazione richiesta

La domanda, sottoscritta dal rappresentante legale dell'Amministrazione, in plico chiuso con evidenza del mittente e con l'indicazione: "Domanda

per l'iscrizione nell'elenco dei certificatori", va indirizzata e fatta pervenire all'Autorità per l'informatica nella Pubblica Amministrazione, Via Isonzo, 21/b - 00198 Roma.

La consegna può avvenire tramite servizio pubblico o privato, oppure a mano, nei giorni compresi tra il lunedì e il venerdì al seguente orario: dalle ore 09.00 alle ore 13.00 e dalle ore 15.00 alle ore 17.00. In quest'ultimo caso verrà data formale ricevuta di consegna del plico.

La domanda e i documenti prodotti dal richiedente, vanno predisposti utilizzando un sistema di elaborazione testi di larga diffusione. Un supporto informatico, contenente tale testo, con l'eccezione del piano per la sicurezza, va allegato alla domanda, insieme alla stampa, in duplice copia, del contenuto del supporto stesso.

La domanda deve recare:

- l'indicazione e la sede dell'Amministrazione;
- l'organo che ne ha la rappresentanza legale;
- l'elenco dei documenti allegati.

È opportuno che vengano indicati il nominativo della persona cui far riferimento, anche per le vie brevi, e le modalità per contattarla (numeri telefonici, telefax, telex), ai fini di una sollecita definizione delle eventuali problematiche che richiedessero chiarimenti di minore importanza.

Alla domanda vanno allegati:

a) copia della certificazione di qualità dei processi informatici e dei relativi prodotti cui all'art. 8, comma 3, lettera d), del d.P.C.M. 8 febbraio 1999;

b) dichiarazione di piena disponibilità a consentire accessi presso le strutture dedicate alle operazioni di certificazione, da parte di incaricati dell'AIPA, per la verifica del mantenimento della rispondenza ai requisiti tecnico-organizzativi di cui alla documentazione allegata alla domanda;

c) copia del manuale operativo;

d) copia del piano per la sicurezza;

e) una relazione sulla struttura organizzativa;

f) dichiarazione di impegno a comunicare tempestivamente all'AIPA ogni variazione significativa delle soluzioni tecnico-organizzative adottate, fermo restando quanto prescritto dall'art.18 del d.P.C.M. 8 febbraio 1999.

2.2. Requisiti tecnico-organizzativi da documentare

2.2.1. Manuale operativo.

Il manuale operativo va strutturato in modo tale da essere integralmente consultabile per via telematica, come prescritto dall'art. 45, comma 2, del d.P.C.M. 8 febbraio 1999.

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;

j) modalità di sospensione e revoca dei certificati;

k) modalità di sostituzione delle chiavi;

l) modalità di gestione del registro dei certificati;

m) modalità di accesso al registro dei certificati;

n) modalità di protezione della riservatezza.

2.2.2. Piano per la sicurezza

Il documento contenente il piano per la sicurezza, in quanto coperto da riservatezza, deve essere racchiuso in una busta sigillata, all'interno del plico contenente la domanda, con evidenza dell'Amministrazione e l'indicazione "Piano per la sicurezza – versione del….(data)".

Il piano deve contenere almeno i seguenti elementi:

a) struttura generale, modalità operativa e struttura logistica dell'organizzazione;

b) descrizione sommaria dell'infrastruttura di sicurezza per ciascun immobile;

c) breve descrizione dell'allocazione degli impianti informatici, dei servizi e degli uffici negli immobili dell'organizzazione;

d) elenco del personale addetto;

e) attribuzioni dettagliate delle responsabilità;

f) algoritmi crittografici utilizzati;

g) descrizione delle procedure utilizzate nell'attività di certificazione, con particolare riferimento ai problemi di sicurezza, alla gestione del log-file e alla garanzia della sua integrità

h) descrizione dei dispositivi di sicurezza installati;

i) descrizione dei flussi di dati;

j) procedura di gestione delle copie di sicurezza dei dati (modalità e frequenze dei salvataggi, tipo e ubicazione delle sicurezze fisiche in conformità alle regole tecniche per l'uso di supporti ottici - deliberazione AIPA n. 24/98);

k) procedure di gestione dei disastri (precisare i tipi di disastri per i quali sono state previste delle soluzioni: per calamità naturali, per dolo, per indisponibilità prolungata del sistema, per altre ragioni; descrivere le soluzioni con dettagli sui tempi e le modalità previste per il ripristino del servizio);

l) analisi dei rischi (precisare i tipi di rischi: per dolo, per infedeltà del personale, per inefficienza operativa, per inadeguatezza tecnologica, per altre ragioni);

m) descrizione delle contromisure (precisare i tempi di reazioni previsti e i nomi dei responsabili);

n) specificazione dei controlli (precisare se è previsto il ricorso periodico a ispezioni esterne).

2.2.3. Organizzazione del personale

Deve essere predisposto un apposito documento contenente la descrizione dell'organizzazione del personale, limitatamente alle funzioni elencate nell'art. 49 del d.P.C.M. dell'8 febbraio 1999; tale atto deve essere corredato da un'adeguata documentazione, a norma dell'art. 51 del medesimo decreto, dell'esperienza maturata dal personale stesso.

A norma dell'art. 16, comma 2, del citato d.P.C.M., deve essere precisato, in particolare, il profilo del personale responsabile delle generazioni delle chiavi, della emissione dei certificati e della gestione del

registro delle chiavi. Tale profilo dovrà essere idoneo ad attestare il possesso della competenza e dell'esperienza richiesti dall'art. 8, comma 3, lettera c), del d.P.R. 10 novembre 1997, n. 513.

2.3. Requisiti tecnico-organizzativi da autocertificare.

L'Amministrazione è tenuta a specificare, con apposita dichiarazione, i punti che seguono:

a) algoritmi di generazione e verifica firme utilizzati e supportati;

b) algoritmi di hash utilizzati e supportati;

c) lunghezza delle chiavi;

d) assicurazioni relative al sistema di generazione delle chiavi;

e) caratteristiche del sistema di generazione;

f) informazioni contenute nei certificati;

g) formato dei certificati;

h) modalità di accesso al registro dei certificati;

i) modalità con la quale viene soddisfatta la verifica dell'unicità della chiave pubblica, in rapporto allo stato delle conoscenze scientifiche e tecnologiche;

j) caratteristiche del sistema di generazione dei certificati;

k) modalità di attuazione della copia del registro dei certificati;

l) modalità di tenuta del giornale di controllo;

m) descrizione del sistema di validazione temporale adottato;

n) impegno ad adottare ogni opportuna misura tecnico-organizzativa volta a garantire il rispetto delle disposizioni della legge 31 dicembre 1996, n. 675.

E' data facoltà di limitare la documentazione alle sole informazioni non soggette a particolari ragioni di riservatezza. L'AIPA, dal canto suo, si riserva, a norma dell'art. 16, comma 3, del d.P.C.M. dell'8 febbraio 1999, di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato.

2.4. Modalità di esame delle domande.

L'istruttoria sulle domande e sulla relativa documentazione sarà svolta, sotto il controllo di un membro dell'Autorità per l'informatica all'uopo

designato, a cura degli Uffici, con la concordata collaborazione specialistica del Centro tecnico di cui all'art. 17, comma 19, della legge 15 maggio 1997, n. 127. Al termine dell'istruttoria sulla richiesta di iscrizione nell'elenco pubblico dei certificatori, sarà adottata dall'Autorità, su proposta formulata dal Membro designato, deliberazione motivata di accoglimento o di reiezione ovvero di integrazione dell'istruttoria, se ritenuta necessaria.

In caso di reiezione della domanda di iscrizione, l'amministrazione interessata non può presentare una nuova istanza, se non siano trascorsi almeno sei mesi dalla data di comunicazione del provvedimento stesso e, comunque, prima che siano cessate le cause che hanno determinato il non accoglimento della domanda.

Eventuali richieste di delucidazioni e/o chiarimenti potranno essere inoltrate al Direttore generale dell'Autorità per l'informatica.

3. Sottoscrizione del documento informatico con modalità semplificate (sub punto b).

La sottoscrizione prevista al punto sub b) è finalizzata a soddisfare esigenze di semplificazione del processo di formazione dei documenti amministrativi, per quegli adempimenti di rilevanza esclusivamente interna, ritenendosi che l'impiego della firma digitale, come prevista dal DPR n. 513/97 e dalle relative regole tecniche, contenute nel d.P.C.M. dell'8 febbraio 1999, determinerebbe un notevole appesantimento del processo documentale stesso.

Ogni amministrazione pubblica potrà prescindere dal formale processo di certificazione della chiave pubblica previsto dal d.P.R. n. 513/97 e dal d.P.C.M. 8 febbraio 1999 e ricorrere a regole tecniche dalla stessa autonomamente definite, sia per la generazione e conservazione delle chiavi pubbliche che per la loro certificazione, limitatamente alla sottoscrizione dei documenti informatici d'uso interno e con riferimento al proprio ordinamento.

Per tali adempimenti, la deroga alle regole tecniche di cui al d.P.C.M. dell'8 febbraio 1999 è motivata dalla circostanza che la verifica dell'autenticità ed integrità del documento informatico può avvenire attraverso il solo riscontro interno, grazie al processo di certificazione operato da ogni singola amministrazione.

4. Utilizzo di sistemi di identificazione

Gli strumenti di identificazione ed autenticazione, intesi come meccanismi di verifica della reale identità dell'utente, possono essere implementati e gestiti per garantire l'accesso a sistemi o per la produzione di documentazione che non necessiti della sottoscrizione. Le

Amministrazioni, per la definizione delle specifiche di progetto, di implementazione di tali strumenti e di sicurezza si avvalgono di quanto prescritto dal DPR 428/98 e dalle relative regole tecniche nonchè dalle “Linee guida per la definizione di un piano per la sicurezza” emesse dall’AIPA e pubblicate nei Quaderni AIPA n. 2 dell'ottobre 1999 e consultabili sul sito www.aipa.it.

In particolare, è opportuno che tali strumenti costituiscano parte integrante di un insieme di misure finalizzate al raggiungimento degli obiettivi di sicurezza.

Tra le misure adottabili, al fine di cui sopra, sono da ritenere indispensabili:

- la definizione di profili di accesso associati alle utenze definite;
- la verifica dell’integrità dei dati;
- la registrazione, in appositi file di log, delle attività svolte;
- la periodica analisi delle suddette registrazioni.

È inoltre necessario integrare nel sistema di sicurezza le misure previste dal D.P.R. 28 luglio 1999, n. 318, recante norme per l’individuazione delle misure minime di sicurezza per il trattamento dei dati personali a norma dell’art. 15, comma 2, della legge 31 dicembre 1996, n. 675.

*** * * * ***

Si segnala, infine, che le pubbliche amministrazioni:

a) definiscono e gestiscono, in modo autonomo, tutti i processi di identificazione o autenticazione interni alle pubbliche amministrazioni stesse e, comunque, relativi ai propri organi ed uffici;

b) devono accettare tutti i documenti informatici formati e sottoscritti secondo quanto stabilito dal d.P.R. 10 novembre 1997, n. 513, dalle regole tecniche di cui al d.P.C.M. dell’8 febbraio 1999 e dalle regole di interoperabilità definite dalla Circolare AIPA/CR/24 del 19 giugno 2000, in quanto validi e rilevanti ad ogni effetto di legge;

c) devono adottare i principi di interoperabilità definiti dalla citata circolare AIPA/CR/24.

Il Presidente: REY