

Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Gazz. Uff. n. 60 del 13 marzo 1998)

Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59.

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87 della Costituzione;

Visto l'articolo 17, comma 2, della legge 23 agosto 1988 n. 400;

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

Visto il decreto legislativo 12 febbraio 1993, n.39;

Sentito il Garante per la protezione dei dati personali;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 5 agosto 1997;

Acquisiti i pareri delle commissioni permanenti della Camera dei deputati e del Senato della Repubblica;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 20 ottobre 1997;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 31 ottobre 1997;

Sulla proposta del Presidente del Consiglio dei Ministri e del Ministro per la funzione pubblica e gli affari regionali, di concerto con il Ministro di grazia e giustizia;

EMANA

il seguente regolamento:

Capo I - PRINCIPI GENERALI

Art. 1.

(Definizioni)

Ai fini del presente regolamento s'intende:

- per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;
- per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;
- per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.
- per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;

- per chiave biometrica, la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente;
- per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;
- per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;
- per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;
- per certificatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;
- per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;
- per sospensione del certificato, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;
- per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;
- per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.

Art. 2. (Documento informatico)

Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.

Art. 3 (Requisiti del documento informatico)

Con decreto del Presidente del Consiglio dei Ministri, da emanare entro 180 giorni dall'entrata in vigore del presente regolamento, sentita l'Autorità per l'informatica nella pubblica amministrazione sono fissate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

Le regole tecniche indicate al comma 1 sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con decorrenza almeno biennale a decorrere dall'entrata in vigore del presente regolamento.

Con il decreto di cui al comma 1 sono altresì dettate le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche.

Resta fermo quanto previsto dall'articolo 15 della legge 31 dicembre 1996, n.675.

Art. 4. (Forma scritta)

Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta.

Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro delle finanze.

Art. 5.
(Efficacia probatoria del documento informatico)

Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.

Il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

Art.6.
(Copie di atti e documenti)

I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento.

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

Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3.

La spedizione o il rilascio di copie di atti e documenti di cui al comma 2 esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 3.

Art. 7
(Deposito della chiave privata)

Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata presso un notaio o altro pubblico depositario autorizzato.

La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e dev'essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni.

Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili.

Art.8.
(Certificazione)

Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 2 deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.

Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro validità, sono consultabili in forma telematica.

Salvo quanto previsto dall'articolo 17, le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 3:

forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;

possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;

affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;

qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

La procedura di certificazione di cui al comma 1 può essere svolta anche da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione europea o dello Spazio economico europeo, sulla base di equivalenti requisiti.

Art. 9. (Obblighi dell'utente e del certificatore)

Chiunque intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il certificatore è tenuto a :

- identificare con certezza la persona che fa richiesta della certificazione;
- rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 3;
- specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;
- attenersi alle regole tecniche di cui all'articolo 3;
- informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
- attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;
- non rendersi depositario di chiavi private;
- procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;
- dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche;
- dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.

CAPO II FIRMA DIGITALE

Art. 10
(Firma digitale)

A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale.

L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.

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

Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata.

L'uso della firma digitale apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

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

Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche definiti con il decreto di cui all'articolo 3, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

Art. 11
(Contratti stipulati con strumenti informatici o per via telematica)

I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge.

Ai contratti indicati al comma 1 si applicano le disposizioni previste dal decreto legislativo 15 gennaio 1992, n.50.

Art. 12
(Trasmissione del documento)

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente regolamento e alle regole tecniche di cui all'articolo 3, sono opponibili ai terzi.

La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Art. 13
(Segretezza della corrispondenza trasmessa per via telematica)

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

Agli effetti del presente regolamento, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Art. 14 (Pagamenti informatici)

Il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art.15 (Libri e scritture)

I libri, i repertori e le scritture, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente regolamento e secondo le regole tecniche definite col decreto di cui all'articolo 3.

Art.16 (Firma digitale autenticata)

Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.

L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, numero 1, della legge 16 febbraio 1913, n. 89 .

L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 6 del presente regolamento.

Ai fini e per gli effetti dell'articolo 3, comma 11, della legge 15 maggio 1997, n. 127, si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.

La presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione sono validi a tutti gli effetti di legge se vi sono apposte la firma digitale e la validazione temporale a norma del presente regolamento.

Art. 17 (Chiavi di cifratura della pubblica amministrazione)

Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.

Col decreto di cui all'articolo 3 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni.

Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente, in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici.

Le chiavi pubbliche di Ordini ed Albi professionali legalmente riconosciuti e dei loro legali rappresentanti sono certificate e pubblicate a cura del Ministro di Grazia e Giustizia o suoi delegati.

Art. 18
(Documenti informatici delle pubbliche amministrazioni)

Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

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

Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dall'Autorità per l'informatica nella pubblica amministrazione d'intesa con l'amministrazione degli archivi di Stato.

Art. 19
(Sottoscrizione dei documenti informatici delle pubbliche amministrazioni)

In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa, o la sottoscrizione comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente regolamento.

L'uso della firma digitale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

CAPO III
NORME DI ATTUAZIONE

Art.20
(Sviluppo dei sistemi informativi delle pubbliche amministrazioni)

Entro il 31 marzo 1998 le pubbliche amministrazioni adottano un piano di sviluppo dei sistemi informativi automatizzati in attuazione delle disposizioni del presente regolamento e secondo le norme tecniche definite dall'Autorità per l'informatica nella pubblica amministrazione.

Le pubbliche amministrazioni provvedono, entro 5 anni, a partire dal 1 gennaio 1998, a realizzare o revisionare sistemi informativi finalizzati alla totale automazione delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti in conformità alle disposizioni del presente regolamento ed alle disposizioni di cui alle leggi 31 dicembre 1996, nn. 675 e 676.

Entro il 31 dicembre 1998, le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia opportuna od obbligatoria la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici.

Art. 21
(Gestione informatica del flusso documentale)

Entro il 31 dicembre 1998 le pubbliche amministrazioni dispongono per la tenuta del protocollo amministrativo e per la gestione dei documenti con procedura informatica al fine di consentire il reperimento immediato, la disponibilità degli atti archiviati e l'accesso ai documenti amministrativi per via telematica tra pubbliche amministrazioni e tra queste ed i soggetti privati aventi diritto.

Art. 22
(Formulari, moduli e questionari)

Entro il 31 dicembre 1998 le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge per l'interscambio dei dati nell'ambito della rete unitaria e con i soggetti privati.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella *Raccolta ufficiale* degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo o di farlo osservare.