

**TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E
REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE
AMMINISTRATIVA**

LEGENDA:

L: legge

R: regolamento

SCHEMA DI TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE AMMINISTRATIVA

IL PRESIDENTE DELLA REPUBBLICA

VISTO gli articoli 76 e 87, comma quinto, della Costituzione;

VISTO gli articoli 14, 16 e 17, comma 2, della legge 23 agosto 1988, n.400;

VISTA l'articolo 7 della legge 8 marzo 1999, n.50;

VISTO il punto 4) dell'allegato 3, della legge 8 marzo 1999, n.50;

VISTA le risoluzioni del Senato della Repubblica del 24 novembre 1999 e della Camera dei deputati 19 novembre 1999;

VISTO il decreto legislativo.....;

VISTO il decreto del Presidente della Repubblica.....;

VISTE le deliberazioni preliminari del Consiglio dei Ministri adottate nelle riunioni del 25 agosto 2000 e del 06 ottobre 2000;

VISTO il parere della Conferenza Stato-città, ai sensi dell'articolo 8 del decreto legislativo 28 agosto 1997 n.281, espresso nella riunione del 14 settembre 2000;

UDITO il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 18 settembre 2000;

ACQUISITO il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei Ministri adottata nella riunione del

SULLA PROPOSTA del Presidente del Consiglio dei Ministri e del Ministro per la funzione pubblica, di concerto con i Ministri dell'interno e della giustizia;

EMANA

il seguente testo unico:

TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE AMMINISTRATIVA

CAPO I

DEFINIZIONI E AMBITO DI APPLICAZIONE

Articolo 1 (R)

Definizioni

1. Ai fini del presente testo unico si intende per:

- a) DOCUMENTO AMMINISTRATIVO ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Le relative modalità di trasmissione sono quelle indicate al capo II, sezione III del presente testo unico.
- b) DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- c) DOCUMENTO DI RICONOSCIMENTO ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consente l'identificazione personale del titolare.
- d) DOCUMENTO D'IDENTITÀ la carta di identità ed ogni altro documento munito di fotografia rilasciato, su supporto cartaceo, magnetico o informatico, dall'amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare.
- e) DOCUMENTO D'IDENTITÀ ELETTRONICO il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età.
- f) CERTIFICATO il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione e partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche.**
- g) DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE il documento, sottoscritto dall'interessato, prodotto in sostituzione dei certificati di cui alla lettera f).

h) DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA' il documento, sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal presente testo unico.

i) AUTENTICAZIONE DI SOTTOSCRIZIONE l'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive.

l) LEGALIZZAZIONE DI FIRMA l'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa.

m) LEGALIZZAZIONE DI FOTOGRAFIA l'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato.

n) 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.

o) AMMINISTRAZIONI PROCEDENTI le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive di cui alle lettere g) e h) o provvedono agli accertamenti d'ufficio ai sensi dell'art. 43.

p) AMMINISTRAZIONI CERTIFICANTI le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti ai sensi degli articoli 43 e 71.

q) GESTIONE DEI DOCUMENTI l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati.

r) SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti.

s) SEGNAZIONE DI PROTOCOLLO l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

Articolo 2 (L)

Oggetto

1. Le norme del presente testo unico disciplinano la formazione, il rilascio, la tenuta e la conservazione, la gestione, la trasmissione di atti e documenti da parte di organi della pubblica amministrazione; disciplinano altresì la produzione di atti e documenti agli organi della pubblica amministrazione nonché ai gestori di pubblici servizi nei rapporti tra loro e in quelli con l'utenza, e ai privati che vi consentono. Le norme concernenti i documenti informatici e la firma digitale, contenute nel capo II, si applicano anche nei rapporti tra privati come previsto dall'articolo 15, comma 2 della legge 15 marzo 1997, n. 59.

Articolo 3 (R)

Soggetti

1. Le disposizioni del presente testo unico si applicano ai cittadini italiani e dell'Unione europea, alle persone giuridiche, alle società di persone, alle pubbliche amministrazioni e agli enti, alle associazioni e ai comitati aventi sede legale in Italia o in uno dei Paesi dell'Unione europea. **(R)**

2. I cittadini di Stati non appartenenti all'Unione regolarmente soggiornanti in Italia, possono utilizzare le dichiarazioni sostitutive di cui agli articoli 46 e 47 limitatamente agli stati, alle qualità personali e ai fatti certificabili o attestabili da parte di soggetti pubblici italiani, fatte salve le speciali disposizioni contenute nelle leggi e nei regolamenti concernenti la disciplina dell'immigrazione e la condizione dello straniero. **(R)**

3. Al di fuori dei casi previsti al comma 2, i cittadini di Stati non appartenenti all'Unione autorizzati a soggiornare nel territorio dello Stato possono utilizzare le dichiarazioni sostitutive di cui agli articoli 46 e 47 nei casi in cui la produzione delle stesse avvenga in applicazione di convenzioni internazionali fra l'Italia ed il Paese di provenienza del dichiarante. **(R)**

4. Al di fuori dei casi di cui ai commi 2 e 3 gli stati, le qualità personali e i fatti, sono documentati mediante certificati o attestazioni rilasciati dalla competente autorità dello Stato estero, corredati di traduzione in lingua italiana autenticata dall'autorità consolare italiana che ne attesta la conformità all'originale, dopo aver

ammonito l'interessato sulle conseguenze penali della produzione di atti o documenti non veritieri.

Articolo 4 (R)

Impedimento alla sottoscrizione e alla dichiarazione

1. La dichiarazione di chi non sa o non può firmare è raccolta dal pubblico ufficiale previo accertamento dell'identità del dichiarante. Il pubblico ufficiale attesta che la dichiarazione è stata a lui resa dall'interessato in presenza di un impedimento a sottoscrivere. **(R)**
2. La dichiarazione nell'interesse di chi si trovi in una situazione di impedimento temporaneo, per ragioni connesse allo stato di salute, è sostituita dalla dichiarazione, contenente espressa indicazione dell'esistenza di un impedimento, resa dal coniuge o, in sua assenza, dai figli o, in mancanza di questi, da altro parente in linea retta o collaterale fino al terzo grado, al pubblico ufficiale, previo accertamento dell'identità del dichiarante. **(R)**
3. Le disposizioni del presente articolo non si applicano in materia di dichiarazioni fiscali. **(R)**

Articolo 5 (L)

Rappresentanza legale

1. Se l'interessato è soggetto alla potestà dei genitori, a tutela, o a curatela, le dichiarazioni e i documenti previsti dal presente testo unico sono sottoscritti rispettivamente dal genitore esercente la potestà, dal tutore, o dall'interessato stesso con l'assistenza del curatore.

CAPO II

DOCUMENTAZIONE AMMINISTRATIVA

SEZIONE I

DOCUMENTI AMMINISTRATIVI E ATTI PUBBLICI

Articolo 6 (L-R)

Riproduzione e conservazione di documenti

1. Le pubbliche amministrazioni ed i privati hanno facoltà di sostituire, a tutti gli effetti, i documenti dei propri archivi, le scritture contabili, la corrispondenza e gli altri atti di cui per legge o regolamento è prescritta la conservazione, con la loro riproduzione su supporto fotografico, su supporto ottico o con altro mezzo idoneo a garantire la conformità dei documenti agli originali. **(L)**
2. Gli obblighi di conservazione ed esibizione dei documenti di cui al comma 1 si intendono soddisfatti, sia ai fini amministrativi che probatori, anche se realizzati su supporto ottico quando le procedure utilizzate sono conformi alle regole tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione. **(L)**
3. I limiti e le modalità tecniche della riproduzione e dell'autenticazione dei documenti di cui al comma 1, su supporto fotografico o con altro mezzo tecnico idoneo a garantire la conformità agli originali, sono stabiliti con decreto del Presidente del Consiglio dei Ministri.
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche e sugli archivi privati dichiarati di notevole interesse storico, ai sensi delle disposizioni del Capo II del decreto legislativo 29 ottobre 1999, n. 490.

Articolo 7 (L)

Redazione e stesura di atti pubblici

1. I decreti, gli atti ricevuti dai notai, tutti gli altri atti pubblici, e le certificazioni sono redatti, anche promiscuamente, con qualunque mezzo idoneo, atto a garantirne la conservazione nel tempo.
2. Il testo degli atti pubblici comunque redatti non deve contenere lacune, aggiunte, abbreviazioni, correzioni, alterazioni o abrasioni. Sono ammesse abbreviazioni, acronimi, ed espressioni in lingua straniera, di uso comune. Qualora risulti necessario apportare variazioni al testo, si provvede in modo che la precedente stesura resti leggibile.

SEZIONE II

DOCUMENTO INFORMATICO

Articolo 8 (R)

Documento informatico

1. Il documento informatico da chiunque formato, la registrazione 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 testo unico.
2. Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definite con decreto del Presidente del Consiglio dei Ministri sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante per la protezione dei dati personali. Esse sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno biennale.
3. Con il medesimo decreto del Presidente del Consiglio dei Ministri sono definite 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 di cui all'articolo 22, lettera e).
4. Restano ferme le disposizioni di legge sulla tutela della riservatezza dei dati personali.

Articolo 9 (R)

Documenti informatici delle pubbliche amministrazioni

1. 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.
2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, 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.

3. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

4. 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 il Ministero per i beni e le attività culturali e, per il materiale classificato, con le Amministrazioni della difesa, dell'interno e delle finanze, rispettivamente competenti.

Articolo 10 (R)

Forma ed efficacia del documento informatico

1. Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 e per le pubbliche amministrazioni, anche di quelle di cui all'articolo 9, comma 4, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile.

2. 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.

3. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.

4. Il documento informatico redatto in conformità alle regole tecniche di cui all'articolo 8, comma 2 soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

Articolo 11 (R)

Contratti stipulati con strumenti informatici o per via telematica

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

2. Ai contratti indicati al comma 1 si applicano le vigenti disposizioni in materia di contratti negoziati al di fuori dei locali commerciali.

Articolo 12 (R)

Pagamenti informatici

1. 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 8, comma 2.

Articolo 13 (R)

Libri e scritture

1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente testo unico e secondo le regole tecniche definite col decreto di cui all'articolo 8, comma 2.

SEZIONE III

TRASMISSIONE DI DOCUMENTI

Articolo 14 (R)

Trasmissione del documento informatico

1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato.
2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi.
3. 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.

Articolo 15 (L)

Trasmissione dall'estero di atti agli uffici di stato civile

1. In materia di trasmissione di atti o copie di atti di stato civile o di dati concernenti la cittadinanza da parte delle rappresentanze diplomatiche e consolari italiane, si osservano le disposizioni speciali sulle funzioni e sui poteri consolari.

Articolo 16 (R)

Riservatezza dei dati personali contenuti nei documenti trasmessi

1. Al fine di tutelare la riservatezza dei dati personali di cui agli articoli 22 e 24 della legge 31 dicembre 1996, n. 675, i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

2. Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita.

3. Ai fini statistici, i direttori sanitari inviano copia del certificato di assistenza al parto, privo di elementi identificativi diretti delle persone interessate, ai competenti enti ed uffici del Sistema statistico nazionale, secondo modalità preventivamente concordate. L'Istituto nazionale di statistica, sentiti il Ministero della sanità e il Garante per la protezione dei dati personali, determina nuove modalità tecniche e procedure per la rilevazione dei dati statistici di base relativi agli eventi di nascita e per l'acquisizione dei dati relativi ai nati affetti da malformazioni e ai nati morti nel rispetto dei principi contenuti nelle disposizioni di legge sulla tutela della riservatezza dei dati personali.

Articolo 17 (R)

Segretezza della corrispondenza trasmessa per via telematica

1. 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.

2. Agli effetti del presente testo unico, 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.

SEZIONE IV

COPIE AUTENTICHE, AUTENTICAZIONE DI SOTTOSCRIZIONI

Articolo 18 (L-R)

Copie autentiche

1. Le copie autentiche, totali o parziali, di atti e documenti possono essere ottenute con qualsiasi procedimento che dia garanzia della riproduzione fedele e duratura dell'atto o documento. Esse possono essere validamente prodotte in luogo degli originali. **(L)**

2. L'autenticazione delle copie può essere fatta dal pubblico ufficiale dal quale è stato emesso o presso il quale è depositato l'originale, o al quale deve essere prodotto il documento, nonché da un notaio, cancelliere, segretario comunale, o altro funzionario incaricato dal sindaco. Essa consiste nell'attestazione di conformità con l'originale scritta alla fine della copia, a cura del pubblico ufficiale autorizzato, il quale deve altresì indicare la data e il luogo del rilascio, il numero dei fogli impiegati, il proprio nome e cognome, la qualifica rivestita nonché apporre la propria firma per esteso ed il timbro dell'ufficio. Se la copia dell'atto o documento consta di più fogli il pubblico ufficiale appone la propria firma a margine di ciascun foglio intermedio. Per le copie di atti e documenti informatici si applicano le disposizioni contenute nell'articolo 20. **(L)**

3. Nei casi in cui l'interessato debba presentare alle amministrazioni o ai gestori di pubblici servizi copia autentica di un documento, l'autenticazione della copia può essere fatta dal responsabile del procedimento o da qualsiasi altro dipendente competente a ricevere la documentazione, su esibizione dell'originale e senza obbligo di deposito dello stesso presso l'amministrazione procedente. In tal caso la copia autentica può essere utilizzata solo nel procedimento in corso. **(R)**

Articolo 19 (R)

Modalità alternative all'autenticazione di copie

1. La dichiarazione sostitutiva dell'atto di notorietà di cui all'articolo 47 può riguardare anche il fatto che la copia di un atto o di un documento conservato o rilasciato da una pubblica amministrazione, la copia di una pubblicazione ovvero la copia di titoli di studio o di servizio sono conformi all'originale. Tale dichiarazione può altresì riguardare la conformità all'originale della copia dei documenti fiscali che devono essere obbligatoriamente conservati dai privati.

Articolo 20 (R)

Copie di atti e documenti informatici

1. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi alle disposizioni del presente testo unico.
2. 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 testo unico.
3. 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 secondo le regole tecniche di cui all'articolo 8, comma 2.
4. 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.
5. 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 nell'articolo 8, comma 2.

Articolo 21 (R)

Autenticazione delle sottoscrizioni

1. L'autenticità della sottoscrizione di qualsiasi istanza o dichiarazione sostitutiva di atto di notorietà da produrre agli organi della pubblica amministrazione, nonché ai gestori di servizi pubblici è garantita con le modalità di cui all'art. 38, comma 2 e comma 3. **(R)**

2. Se l'istanza o la dichiarazione sostitutiva di atto di notorietà è presentata a soggetti diversi da quelli indicati al comma 1 o a questi ultimi al fine della riscossione da parte di terzi di benefici economici, l'autenticazione è redatta da un notaio, cancelliere, segretario comunale, dal dipendente addetto a ricevere la documentazione o altro dipendente incaricato dal Sindaco; in tale ultimo caso, l'autenticazione è redatta di seguito alla sottoscrizione e il pubblico ufficiale, che autentica, attesta che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità del dichiarante, indicando le modalità di identificazione, la data ed il luogo di autenticazione, il proprio nome, cognome e la qualifica rivestita, nonché apponendo la propria firma e il timbro dell'ufficio. **(R)**

SEZIONE V

FIRMA DIGITALE

Articolo 22 (R)

Definizioni

1. Ai fini del presente Testo unico si intende:

- a) per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;
- b) 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;

- c) 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;
- d) 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;
- e) 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;
- f) 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;
- g) 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;
- h) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;
- i) 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;
- l) per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;
- m) per sospensione del certificato, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;
- n) per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;
- o) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.

Articolo 23 (R)

Firma digitale

1. 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.
2. 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.
3. 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.
4. 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.
5. L'uso della firma 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.
6. 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.
7. Attraverso la firma digitale devono potersi rilevare nei modi e con le tecniche definiti con il decreto di cui all'articolo 8, comma 2, 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.

Articolo 24 (R)

Firma digitale autenticata

1. 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.
2. 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, primo comma, n.1 della legge 6 febbraio 1913, n.89.

3. 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.

4. 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 20, comma 3.

5. Ai fini e per gli effetti della presentazione di istanze agli organi della pubblica amministrazione si considera apposta in presenza del dipendente addetto la firma digitale inserita nel documento informatico presentato o depositato presso pubbliche amministrazioni.

6. 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 testo unico.

Articolo 25 (R)

Firma di documenti informatici delle pubbliche amministrazioni

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

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

Articolo 26 (R)

Deposito della chiave privata

1. 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.

2. La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e deve essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni.
3. Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili.

Articolo 27 (R)

Certificazione delle chiavi

1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 8, comma 1 deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.
2. 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 valutabilità, sono consultabili in forma telematica.
3. Salvo quanto previsto dall'articolo 29, 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 con il decreto di cui all'articolo 8, comma 2:
 - a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;
 - b) 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;
 - c) 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 testo unico e le regole tecniche di cui all'articolo 8, comma 2;
 - d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.
4. 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.

Articolo 28 (R)

Obblighi dell'utente e del certificatore

1. 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.

2. Il certificatore è tenuto a:

- a) identificare con certezza la persona che fa richiesta della certificazione;
- b) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 8, comma 2;
- c) 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;
- d) attenersi alle regole tecniche di cui all'articolo 8, comma 2;
- e) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
- f) 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;
- g) non rendersi depositario di chiavi private;
- h) 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;
- i) dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche;
- l) 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.

Articolo 29 (R)

Chiavi di cifratura della pubblica amministrazione

1. Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.
2. Con il decreto di cui all'articolo 8 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni.
3. 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.
4. Le chiavi pubbliche di ordini ed albi professionali legalmente riconosciuti e dei loro legali rappresentanti sono certificate e pubblicate a cura del Ministro della giustizia o suoi delegati.

SEZIONE VI

LEGALIZZAZIONE DI FIRME E DI FOTOGRAFIE

Articolo 30 (L)

Modalità per la legalizzazione di firme

1. Nelle legalizzazioni devono essere indicati il nome e il cognome di colui la cui firma si legalizza. Il pubblico ufficiale legalizzante deve indicare la data e il luogo della legalizzazione, il proprio nome e cognome, la qualifica rivestita, nonché apporre la propria firma per esteso ed il timbro dell'ufficio.

Articolo 31 (L)

Atti non soggetti a legalizzazione

1. Salvo quanto previsto negli articoli 32 e 33, non sono soggette a legalizzazione le firme apposte da pubblici funzionari o pubblici ufficiali su atti, certificati, copie ed estratti dai medesimi rilasciati. Il funzionario o pubblico ufficiale deve indicare la data e il luogo del rilascio, il proprio nome e cognome, la qualifica rivestita, nonché apporre la propria firma per esteso ed il timbro dell'ufficio.

Articolo 32 (L)

Legalizzazione di firme di capi di scuole parificate o legalmente riconosciute

1. Le firme dei capi delle scuole parificate o legalmente riconosciute sui diplomi originali o sui certificati di studio da prodursi ad uffici pubblici fuori della provincia in cui ha sede la scuola sono legalizzate dal provveditore agli studi.

Articolo 33 (L)

Legalizzazione di firme di atti da e per l'estero

1. Le firme sugli atti e documenti formati nello Stato e da valere all'estero davanti ad autorità estere sono, ove da queste richiesto, legalizzate a cura dei competenti organi, centrali o periferici, del Ministero competente, o di altri organi e autorità delegati dallo stesso.

2. Le firme sugli atti e documenti formati all'estero da autorità estere e da valere nello Stato sono legalizzate dalle rappresentanze diplomatiche o consolari italiane all'estero. Le firme apposte su atti e documenti dai competenti organi delle rappresentanze diplomatiche o consolari italiane o dai funzionari da loro delegati non sono soggette a legalizzazione. Si osserva l'articolo 31.

3. Agli atti e documenti indicati nel comma precedente, redatti in lingua straniera, deve essere allegata una traduzione in lingua italiana certificata conforme al testo straniero dalla competente rappresentanza diplomatica o consolare, ovvero da un traduttore ufficiale.

4. Le firme sugli atti e documenti formati nello Stato e da valere nello Stato, rilasciati da una rappresentanza diplomatica o consolare estera residente nello Stato, sono legalizzate a cura delle prefetture.

5. Sono fatte salve le esenzioni dall'obbligo della legalizzazione e della traduzione stabilite da leggi o da accordi internazionali.

Articolo 34 (L)

Legalizzazione di fotografie

1. Le amministrazioni competenti per il rilascio di documenti personali sono tenute a legalizzare le prescritte fotografie presentate personalmente dall'interessato. Su richiesta di quest'ultimo le fotografie possono essere, altresì, legalizzate dal dipendente incaricato dal Sindaco.

2. La legalizzazione delle fotografie prescritte per il rilascio dei documenti personali non è soggetta all'obbligo del pagamento dell'imposta di bollo.

SEZIONE VII

DOCUMENTI DI RICONOSCIMENTO E DI IDENTITÀ

Articolo 35 (L -R)

Documenti di identità e di riconoscimento

1. In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2. **(R)**

2. Sono equipollenti alla carta di identità il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato. **(R)**

3. Nei documenti d'identità e di riconoscimento non è necessaria l'indicazione o l'attestazione dello stato civile, salvo specifica istanza del richiedente. **(L)**

Articolo 36 (L)

Carta d'identità e documenti elettronici

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e del documento d'identità elettronico sono definite con decreto del Presidente del Consiglio dei Ministri su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, sentito il Garante per la protezione dei dati personali.

2. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno, devono contenere:

- a) i dati identificativi della persona;
- b) il codice fiscale;

3. La carta d'identità e il documento elettronico possono contenere:

- a) l'indicazione del gruppo sanguigno;
- b) le opzioni di carattere sanitario previste dalla legge;
- c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;
- d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;
- e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti ivi compresa la chiave biometrica, occorrenti per la firma digitale.

4. La carta d'identità elettronica può altresì essere utilizzata per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni.

5. Con decreto del Ministro dell'interno, sentiti l'Autorità per l'informatica nella pubblica amministrazione, il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione delle carte di identità e dei documenti di riconoscimento di cui al presente articolo. Le predette regole sono adeguate con cadenza almeno biennale in relazione alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche.

6. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità

di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.

7. La carta di identità, ancorché su supporto cartaceo, può essere rinnovata a decorrere dal centottantesimo giorno precedente la scadenza.

SEZIONE VIII

REGIME FISCALE

Articolo 37 (L)

Esenzioni fiscali

1. Le dichiarazioni sostitutive di cui agli articoli 46 e 47 sono esenti dall'imposta di bollo.
2. L'imposta di bollo non è dovuta quando per le leggi vigenti sia esente da bollo l'atto sostituito ovvero quello nel quale è apposta la firma da legalizzare.

CAPO III

SEMPLIFICAZIONE DELLA DOCUMENTAZIONE AMMINISTRATIVA

SEZIONE I

ISTANZE E DICHIARAZIONI DA PRESENTARE ALLA PUBBLICA AMMINISTRAZIONE

Articolo 38 (L-R)

Modalità di invio e sottoscrizione delle istanze

1. Tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica. **(L)**
2. Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale o quando il sottoscrittore è identificato dal sistema informatico con l'uso della carta di identità elettronica. **(R)**
3. Le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e

presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate per via telematica; nei procedimenti di aggiudicazione di contratti pubblici, detta facoltà è consentita nei limiti stabiliti dal regolamento di cui all'articolo 15, comma 2 della legge 15 marzo 1997, n.59. **(L)**

Articolo 39 (L)

Domande per la partecipazione a concorsi pubblici

1. La sottoscrizione delle domande per la partecipazione a selezioni per l'assunzione, a qualsiasi titolo, in tutte le pubbliche amministrazioni, nonché ad esami per il conseguimento di abilitazioni, diplomi o titoli culturali non è soggetta ad autenticazione.

SEZIONE II

CERTIFICATI

Articolo 40 (L)

Certificazioni contestuali

1. Le certificazioni da rilasciarsi da uno stesso ufficio in ordine a stati, qualità personali e fatti, concernenti la stessa persona, nell'ambito del medesimo procedimento, sono contenute in un unico documento.

Articolo 41 (L)

Validità dei certificati

1. I certificati rilasciati dalle pubbliche amministrazioni attestanti stati, qualità personali e fatti non soggetti a modificazioni hanno validità illimitata. Le restanti certificazioni hanno validità di sei mesi dalla data di rilascio se disposizioni di legge o regolamentari non prevedono una validità superiore.

2. I certificati anagrafici, le certificazioni dello stato civile, gli estratti e le copie integrali degli atti di stato civile sono ammessi dalle pubbliche amministrazioni nonché dai gestori o esercenti di pubblici servizi anche oltre i termini di validità nel caso in cui l'interessato dichiara, in fondo al documento, che le informazioni contenute nel certificato stesso non hanno subito variazioni dalla data di rilascio. Il procedimento per il quale gli atti certificativi sono richiesti deve avere comunque corso, una volta acquisita la dichiarazione dell'interessato. Resta ferma la facoltà di verificare la veridicità e la autenticità delle attestazioni prodotte. In caso di falsa dichiarazione si applicano le disposizioni di cui all'articolo 76.

Articolo 42 (R)

Certificati di abilitazione

1. Tutti i titoli di abilitazione rilasciati al termine di corsi di formazione o di procedimenti autorizzatori all'esercizio di determinate attività, ancorché definiti "certificato", sono denominati rispettivamente "diploma" o "patentino".

SEZIONE III

ACQUISIZIONE DIRETTA DI DOCUMENTI

Articolo 43 (L-R)

Accertamenti d'ufficio

1. Le amministrazioni pubbliche e i gestori di pubblici servizi non possono richiedere atti o certificati concernenti stati, qualità personali e fatti che risultino elencati all'art. 46, che siano attestati in documenti già in loro possesso o che comunque esse stesse siano tenute a certificare. In luogo di tali atti o certificati i soggetti indicati nel presente comma sono tenuti ad acquisire d'ufficio le relative informazioni, previa indicazione, da parte dell'interessato, dell'amministrazione competente e degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti, ovvero ad accettare la dichiarazione sostitutiva prodotta dall'interessato. **(R)**

2. Fermo restando il divieto di accesso a dati diversi da quelli di cui è necessario acquisire la certezza o verificare l'esattezza, si considera operata per finalità di rilevante interesse pubblico, ai fini di quanto previsto dal decreto legislativo 11 maggio 1999, n. 135, la consultazione diretta, da parte di una pubblica

amministrazione o di un gestore di pubblico servizio, degli archivi dell'amministrazione certificante, finalizzata all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive presentate dai cittadini. Per l'accesso diretto ai propri archivi l'amministrazione certificante rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente. **(L)**

3. Quando l'amministrazione procedente opera l'acquisizione d'ufficio ai sensi del precedente comma, può procedere anche per fax e via telematica. **(R)**

4. Al fine di agevolare l'acquisizione d'ufficio di informazioni e dati relativi a stati, qualità personali e fatti, contenuti in albi, elenchi o pubblici registri, le amministrazioni certificanti sono tenute a consentire alle amministrazioni procedenti, senza oneri, la consultazione per via telematica dei loro archivi informatici, nel rispetto della riservatezza dei dati personali. **(R)**

5. In tutti i casi in cui l'amministrazione procedente acquisisce direttamente informazioni relative a stati, qualità personali e fatti presso l'amministrazione competente per la loro certificazione, il rilascio e l'acquisizione del certificato non sono necessari e le suddette informazioni sono acquisite, senza oneri, con qualunque mezzo idoneo ad assicurare la certezza della loro fonte di provenienza. **(R)**

6. I documenti trasmessi da chiunque ad una pubblica amministrazione tramite fax, o con altro mezzo telematico o informatico idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale. **(R)**

Articolo 44 (R)

Acquisizione di estratti degli atti dello stato civile

1. Gli estratti degli atti di stato civile sono richiesti esclusivamente per i procedimenti che riguardano il cambiamento di stato civile e, ove formati o tenuti dagli uffici dello stato civile in Italia o dalle autorità consolari italiane all'estero, vengono acquisiti d'ufficio.

2. Al di fuori delle ipotesi di cui al comma 1 le amministrazioni possono provvedere all'acquisizione d'ufficio degli estratti solo quando ciò sia indispensabile.

SEZIONE IV

ESIBIZIONE DI DOCUMENTO

Articolo 45 (L-R)

Documentazione mediante esibizione

1. I dati relativi a cognome, nome, luogo e data di nascita, la cittadinanza, lo stato civile e la residenza attestati in documenti di identità o di riconoscimento in corso di validità, possono essere comprovati mediante esibizione dei documenti medesimi. È fatto divieto alle amministrazioni pubbliche ed ai gestori o esercenti di pubblici servizi, nel caso in cui all'atto della presentazione dell'istanza sia richiesta l'esibizione di un documento di identità o di riconoscimento, di richiedere certificati attestanti stati o fatti contenuti nel documento esibito. È, comunque, fatta salva per le amministrazioni pubbliche ed i gestori e gli esercenti di pubblici servizi la facoltà di verificare, nel corso del procedimento, la veridicità e l'autenticità dei dati contenuti nel documento di identità o di riconoscimento. **(L)**

2. Nei casi in cui l'amministrazione procedente acquisisce informazioni relative a stati, qualità personali e fatti attraverso l'esibizione da parte dell'interessato di un documento di identità o di riconoscimento in corso di validità, la registrazione dei dati avviene attraverso l'acquisizione della copia fotostatica non autenticata del documento stesso. **(R)**

3. Qualora l'interessato sia in possesso di un documento di identità o di riconoscimento non in corso di validità, gli stati, le qualità personali e i fatti in esso contenuti possono essere comprovati mediante esibizione dello stesso, purché l'interessato dichiari, in calce alla fotocopia del documento, che i dati contenuti nel documento non hanno subito variazioni dalla data del rilascio. **(R)**

SEZIONE V

NORME IN MATERIA DI DICHIARAZIONI SOSTITUTIVE

Articolo 46 (R)

Dichiarazioni sostitutive di certificazioni

1. Sono comprovati con dichiarazioni, anche contestuali all'istanza, sottoscritte dall'interessato e prodotte in sostituzione delle normali certificazioni i seguenti stati, qualità personali e fatti:

- a) data e il luogo di nascita;
- b) residenza;
- c) cittadinanza;
- d) godimento dei diritti civili e politici;
- e) stato di celibe, coniugato, vedovo o stato libero;
- f) stato di famiglia;
- g) esistenza in vita;
- h) nascita del figlio, decesso del coniuge, dell'ascendente o discendente;
- i) iscrizione in albi, registri o elenchi tenuti da pubbliche amministrazioni;
- l) appartenenza a ordini professionali;
- m) titolo di studio, esami sostenuti;
- n) qualifica professionale posseduta, titolo di specializzazione, di abilitazione, di formazione, di aggiornamento e di qualificazione tecnica;
- o) situazione reddituale o economica anche ai fini della concessione dei benefici di qualsiasi tipo previsti da leggi speciali;
- p) assolvimento di specifici obblighi contributivi con l'indicazione dell'ammontare corrisposto;
- q) possesso e numero del codice fiscale, della partita IVA e di qualsiasi dato presente nell'archivio dell'anagrafe tributaria;
- r) stato di disoccupazione;
- s) qualità di pensionato e categoria di pensione;
- t) qualità di studente;
- u) qualità di legale rappresentante di persone fisiche o giuridiche, di tutore, di curatore e simili;
- v) iscrizione presso associazioni o formazioni sociali di qualsiasi tipo;
- z) tutte le situazioni relative all'adempimento degli obblighi militari, ivi comprese quelle attestate nel foglio matricolare dello stato di servizio;
- aa) di non aver riportato condanne penali e di non essere destinatario di provvedimenti che riguardano l'applicazione di misure di prevenzione, di decisioni

civili e di provvedimenti amministrativi iscritti nel casellario giudiziale ai sensi della vigente normativa;

bb) di non essere a conoscenza di essere sottoposto a procedimenti penali;

cc) qualità di vivenza a carico;

dd) tutti i dati a diretta conoscenza dell'interessato contenuti nei registri dello stato civile;

ee) di non trovarsi in stato di liquidazione o di fallimento e di non aver presentato domanda di concordato.

(R)

Articolo 47 (R)

Dichiarazioni sostitutive dell'atto di notorietà

1. L'atto di notorietà concernente stati, qualità personali o fatti che siano a diretta conoscenza dell'interessato è sostituito da dichiarazione resa e sottoscritta dal medesimo con la osservanza delle modalità di cui all'articolo 38. **(R)**

2. La dichiarazione resa nell'interesse proprio del dichiarante può riguardare anche stati, qualità personali e fatti relativi ad altri soggetti di cui egli abbia diretta conoscenza. **(R)**

3. Fatte salve le eccezioni espressamente previste per legge, nei rapporti con la pubblica amministrazione e con i concessionari di pubblici servizi, tutti gli stati, le qualità personali e i fatti non espressamente indicati nell'articolo 46 sono comprovati dall'interessato mediante la dichiarazione sostitutiva di atto di notorietà. **(R)**

4. Salvo il caso in cui la legge preveda espressamente che la denuncia all'Autorità di Polizia Giudiziaria è presupposto necessario per attivare il procedimento amministrativo di rilascio del duplicato di documenti di riconoscimento o comunque attestanti stati e qualità personali dell'interessato, lo smarrimento dei documenti medesimi è comprovato da chi ne richiede il duplicato mediante dichiarazione sostitutiva. **(R)**

Articolo 48 (R)

Disposizioni generali in materia di dichiarazioni sostitutive

1. Le dichiarazioni sostitutive hanno la stessa validità temporale degli atti che sostituiscono.

2. Le singole amministrazioni predispongono i moduli necessari per la redazione delle dichiarazioni sostitutive, che gli interessati hanno facoltà di utilizzare. Nei moduli per la presentazione delle dichiarazioni sostitutive le amministrazioni inseriscono il richiamo alle sanzioni penali previste dall'articolo 76, per le ipotesi di falsità in atti e dichiarazioni mendaci ivi indicate. Il modulo contiene anche l'informativa di cui all'articolo 10 della legge 31 dicembre 1996, n. 675.

3. In tutti i casi in cui sono ammesse le dichiarazioni sostitutive, le singole amministrazioni inseriscono la relativa formula nei moduli per le istanze.

Articolo 49 (R)

Limiti di utilizzo delle misure di semplificazione

1. I certificati medici, sanitari, veterinari, di origine, di conformità CE, di marchi o brevetti non possono essere sostituiti da altro documento, salvo diverse disposizioni della normativa di settore.

2. Tutti i certificati medici e sanitari richiesti dalle istituzioni scolastiche ai fini della pratica non agonistica di attività sportive da parte dei propri alunni sono sostituiti con un unico certificato di idoneità alla pratica non agonistica di attività sportive rilasciato dal medico di base con validità per l'intero anno scolastico.

CAPO IV

SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

SEZIONE I

DISPOSIZIONI SULLA GESTIONE INFORMATICA DEI DOCUMENTI

Articolo 50 (R)

Attuazione dei sistemi

1. Le pubbliche amministrazioni provvedono ad introdurre nei piani di sviluppo dei sistemi informativi automatizzati progetti per la realizzazione di sistemi di protocollo informatico in attuazione delle disposizioni del presente testo unico.

2. Le pubbliche amministrazioni predispongono appositi progetti esecutivi per la sostituzione dei registri di protocollo cartacei con sistemi informatici conformi alle disposizioni del presente testo unico.

3. Le pubbliche amministrazioni provvedono entro il 1° gennaio 2004 a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del presente testo unico ed alle disposizioni di legge sulla tutela della riservatezza dei dati personali, nonché dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 e dei relativi regolamenti di attuazione.

4. Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.

5. Le amministrazioni centrali dello Stato provvedono alla gestione informatica dei documenti presso gli uffici di registrazione di protocollo già esistenti alla data di entrata in vigore del presente testo unico presso le direzioni generali e le grandi ripartizioni che a queste corrispondono, i dipartimenti, gli uffici centrali di bilancio, le segreterie di gabinetto.

Articolo 51(R)

Sviluppo dei sistemi informativi delle pubbliche amministrazioni

1. Le pubbliche amministrazioni adottano un piano di sviluppo dei sistemi informativi automatizzati in attuazione delle disposizioni del presente testo unico e secondo le norme tecniche definite dall'Autorità per l'informatica della pubblica amministrazione.

2. Le pubbliche amministrazioni provvedono 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 testo unico ed alle disposizioni di legge sulla tutela della riservatezza dei dati personali.

3. 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 obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici.

Articolo 52 (R)

Il sistema di gestione informatica dei documenti

1. Il sistema di gestione informatica dei documenti, in forma abbreviata "sistema" deve:
- a) garantire la sicurezza e l'integrità del sistema;
 - b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
 - c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
 - d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
 - e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
 - f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Articolo 53 (R)

Registrazione di protocollo

1. La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:
- a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
 - b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
 - c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;

- d) oggetto del documento, registrato in forma non modificabile;
 - e) data e protocollo del documento ricevuto, se disponibili;
 - f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
2. Il sistema deve consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
 3. L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.
 4. Con decreto del Presidente del Consiglio dei Ministri, su proposta dell'Autorità per l'informatica nella pubblica amministrazione di concerto con il Ministro per la funzione pubblica, sono specificate le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione di protocollo.
 5. Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

Articolo 54 (R)

Informazioni annullate o modificate

1. Le informazioni non modificabili di cui all'articolo 53 lett. a), b), c), d), e) e f) sono annullabili con la procedura di cui al presente articolo. Le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura.
2. La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione.

Articolo 55 (R)

Segnatura di protocollo

1. La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:

- a) il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;
- b) la data di protocollo;
- c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4.

2. L'operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione di protocollo.

3. L'operazione di segnatura di protocollo può includere il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo.

4. Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento. L'amministrazione che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

5. Con Decreto del Presidente del Consiglio dei Ministri, su proposta dell'Autorità per l'informatica nella pubblica Amministrazione di concerto con il Ministro per la funzione pubblica, sono stabiliti il formato e la struttura delle informazioni associate al documento informatico ai sensi del comma 4.

Articolo 56 (R)

Operazioni ed informazioni minime del sistema di gestione informatica dei documenti

1. Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni.

Articolo 57 (R)

Numero di protocollo

1. Il numero di protocollo è progressivo e costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare.

SEZIONE SECONDA

ACCESSO AI DOCUMENTI E ALLE INFORMAZIONI DEL SISTEMA

Articolo 58 (R)

Funzioni di accesso ai documenti e alle informazioni del sistema

1. L'accesso al sistema da parte degli utenti appartenenti all'Amministrazione, nonché la ricerca, la visualizzazione e la stampa di tutte le informazioni relative alla gestione dei documenti sono disciplinati dai criteri di abilitazione stabiliti dal responsabile della tenuta del servizio di cui all'articolo 61.

2. La ricerca delle informazioni del sistema è effettuata secondo criteri di selezione basati su tutti i tipi di informazioni registrate. I criteri di selezione possono essere costituiti da espressioni semplici o da combinazioni di espressioni legate tra loro per mezzo di operatori logici. Per le informazioni costituite da testi deve essere possibile la specificazione delle condizioni di ricerca sulle singole parole o parti di parole contenute nel testo.

3. Il sistema deve offrire la possibilità di elaborazioni statistiche sulle informazioni registrate allo scopo di favorire le attività di controllo.

Articolo 59 (R)

Accesso esterno

1. Per l'esercizio del diritto di accesso ai documenti amministrativi, possono essere utilizzate tutte le informazioni del sistema di gestione informatica dei documenti anche mediante l'impiego di procedure applicative operanti al di fuori del sistema e strumenti che consentono l'acquisizione diretta delle informazioni da parte dell'interessato.

2. A tal fine le pubbliche amministrazioni determinano, nel rispetto delle disposizioni di legge sulla tutela della riservatezza dei dati personali, e nell'ambito delle misure organizzative volte ad assicurare il diritto di accesso ai documenti amministrativi i criteri tecnici ed organizzativi per l'impiego, anche per via telematica, del sistema di gestione informatica dei documenti per il reperimento, la visualizzazione e la stampa delle informazioni e dei documenti.

3. Nel caso di accesso effettuato mediante strumenti che consentono l'acquisizione diretta delle informazioni e dei documenti da parte dell'interessato, le misure organizzative e le norme tecniche indicate al comma 2 determinano, altresì, le modalità di identificazione del soggetto anche mediante l'impiego di strumenti informatici per la firma digitale del documento informatico, come disciplinati dal presente testo unico.

4. Nel caso di accesso effettuato da soggetti non appartenenti alla pubblica amministrazione possono utilizzarsi le funzioni di ricerca e di visualizzazione delle informazioni e dei documenti messe a disposizione – anche per via telematica – attraverso gli uffici relazioni col pubblico.

Articolo 60 (R)

Accesso effettuato dalle pubbliche amministrazioni

1. Le pubbliche amministrazioni che, mediante proprie applicazioni informatiche, accedono al sistema di gestione informatica dei documenti delle grandi aree organizzative omogenee di cui al comma 4 dell'articolo 50, adottano le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni.

2. Le pubbliche amministrazioni che accedono ai sistemi di gestione informatica dei documenti attraverso la rete unitaria delle pubbliche amministrazioni utilizzano funzioni minime e comuni di accesso per ottenere le seguenti informazioni:

a) numero e data di registrazione di protocollo dei documenti, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;

b) numero e data di registrazione di protocollo del documento ricevuto, ottenuti attraverso l'indicazione della data e del numero di protocollo attribuiti dall'amministrazione al documento spedito.

3. Ai fini del presente articolo, le pubbliche amministrazioni provvedono autonomamente, sulla base delle indicazioni fornite dall'Autorità per l'informatica nella pubblica amministrazione, alla determinazione dei criteri tecnici ed organizzativi per l'accesso ai documenti e alle informazioni del sistema di gestione informatica dei documenti.

SEZIONE TERZA

TENUTA E CONSERVAZIONE DEL SISTEMA DI GESTIONE DEI DOCUMENTI

Articolo 61 (R)

Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi

1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.

2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.

3. Il servizio svolge i seguenti compiti:

- a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del presente testo unico;
- c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
- d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
- f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
- g) autorizza le operazioni di annullamento di cui all'articolo 54;
- h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

Articolo 62 (R)

Procedure di salvataggio e conservazione delle informazioni del sistema

1. Il responsabile per la tenuta del sistema di gestione informatica dei documenti dispone per la corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.
2. E' consentito il trasferimento su supporto informatico rimovibile delle informazioni di protocollo relative ai fascicoli che fanno riferimento a procedimenti conclusi.
3. Le informazioni trasferite sono sempre consultabili. A tal fine, il responsabile per la tenuta del sistema di gestione informatica dei documenti dispone, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici.

4. Le informazioni relative alla gestione informatica dei documenti costituiscono parte integrante del sistema di indicizzazione e di organizzazione dei documenti che sono oggetto delle procedure di conservazione sostitutiva.

Articolo 63 (R)

Registro di emergenza

1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. **(R)**

2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. **(R)**

3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. **(R)**

4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. **(R)**

5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza. **(R)**

SEZIONE QUARTA

SISTEMA DI GESTIONE DEI FLUSSI DOCUMENTALI

Articolo 64(R)

Sistema di gestione dei flussi documentali

1. Le pubbliche amministrazioni provvedono in ordine alla gestione dei procedimenti amministrativi mediante sistemi informativi automatizzati, valutando i relativi progetti in termini di rapporto tra costi e benefici, sulla base delle indicazioni fornite dall'Autorità per l'informatica nella pubblica amministrazione.

2. I sistemi per la gestione dei flussi documentali che includono i procedimenti amministrativi di cui al comma 1 è finalizzata al miglioramento dei servizi e al potenziamento dei supporti conoscitivi delle amministrazioni secondo i criteri di economicità, di efficacia dell'azione amministrativa e di pubblicità stabiliti dalla legge.

3. Il sistema per la gestione dei flussi documentali include il sistema di gestione informatica dei documenti.

4. Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo.

Articolo 65 (R)

Requisiti del sistema per la gestione dei flussi documentali

1. Oltre a possedere i requisiti indicati all'articolo 52, il sistema per la gestione dei flussi documentali deve :

- a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
- b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
- c) fornire informazioni statistiche sull'attività dell'ufficio;

d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.

Articolo 66 (R)

Specificazione delle informazioni previste dal sistema di gestione dei flussi documentali

1. Le regole tecniche, i criteri e le specifiche delle informazioni previste, delle operazioni di registrazione e del formato dei dati relativi ai sistemi informatici per la gestione dei flussi documentali sono specificate con decreto del Presidente del Consiglio dei Ministri, su proposta dell'Autorità per l'informatica nella pubblica amministrazione di concerto con il Ministro della funzione pubblica.

SEZIONE QUINTA

DISPOSIZIONI SUGLI ARCHIVI

Articolo 67 (R)

Trasferimento dei documenti all'archivio di deposito

1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione. **(R)**

2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. **(R)**

3. Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito. **(R)**

Articolo 68 (R)

Disposizioni per la conservazione degli archivi

1. Il servizio per la gestione dei flussi documentali e degli archivi elabora ed aggiorna il piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni contenute in materia di tutela dei beni culturali e successive modificazioni ed integrazioni.

2. Dei documenti prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.

3. Si applicano in ogni caso, per l'archiviazione e la custodia dei documenti contenenti dati personali, le disposizioni di legge sulla tutela della riservatezza dei dati personali.

Articolo 69 (R)

Archivi storici

1. I documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

SEZIONE SESTA

ATTUAZIONE ED AGGIORNAMENTO DEI SISTEMI

Articolo 70 (R)

Aggiornamenti del sistema

1. Le pubbliche amministrazioni devono assicurare, per ogni aggiornamento del sistema, il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti.

CAPO V

CONTROLLI

Articolo 71 (R)

Modalità dei controlli

1. Le amministrazioni precedenti sono tenute ad effettuare idonei controlli, anche a campione, e in tutti i casi in cui sorgono fondati dubbi, sulla veridicità delle dichiarazioni sostitutive di cui agli articoli 46 e 47. **(R)**
2. I controlli riguardanti dichiarazioni sostitutive di certificazione sono effettuati dall'amministrazione precedente con le modalità di cui all'articolo 43 consultando direttamente gli archivi dell'amministrazione certificante ovvero richiedendo alla medesima, anche attraverso strumenti informatici o telematici, conferma scritta della corrispondenza di quanto dichiarato con le risultanze dei registri da questa custoditi. **(R)**
3. Qualora le dichiarazioni di cui agli articoli 46 e 47 presentino delle irregolarità o delle omissioni rilevabili d'ufficio, non costituenti falsità, il funzionario competente a ricevere la documentazione dà notizia all'interessato di tale irregolarità. Questi è tenuto alla regolarizzazione o al completamento della dichiarazione; in mancanza il procedimento non ha seguito. **(R)**
4. Qualora il controllo riguardi dichiarazioni sostitutive presentate ai privati che vi consentono di cui all'articolo 2, l'amministrazione competente per il rilascio della relativa certificazione, previa definizione di appositi accordi, è tenuta a fornire, su richiesta del soggetto privato corredata dal consenso del dichiarante, conferma scritta, anche attraverso l'uso di strumenti informatici o telematici, della corrispondenza di quanto dichiarato con le risultanze dei dati da essa custoditi. **(R)**

Articolo 72(R)

Responsabilità dei controlli

1. Ai fini dei controlli di cui all'articolo 71 le amministrazioni certificanti individuano e rendono note le misure organizzative adottate per l'efficiente, efficace e tempestiva esecuzione dei controlli medesimi e le modalità per la loro esecuzione. **(R)**
2. La mancata risposta alle richieste di controllo entro trenta giorni costituisce violazione dei doveri d'ufficio. **(R)**

CAPO VI SANZIONI

Articolo 73 (L)

Assenza di responsabilità della pubblica amministrazione

1. Le pubbliche amministrazioni e i loro dipendenti, salvi i casi di dolo o colpa grave, sono esenti da ogni responsabilità per gli atti emanati, quando l'emanazione sia conseguenza di false dichiarazioni o di documenti falsi o contenenti dati non più rispondenti a verità, prodotti dall'interessato o da terzi.

Articolo 74 (L-R)

Violazione dei doveri d'ufficio

1. Costituisce violazione dei doveri d'ufficio la mancata accettazione delle dichiarazioni sostitutive di certificazione o di atto di notorietà rese a norma delle disposizioni del presente testo unico. **(L)**

2. Costituiscono altresì violazioni dei doveri d'ufficio:

- a) la richiesta di certificati o di atti di notorietà nei casi in cui, ai sensi dell'articolo 43, ci sia l'obbligo del dipendente di accettare la dichiarazione sostitutiva; **(R)**
- b) il rifiuto da parte del dipendente addetto di accettare l'attestazione di stati, qualità personali e fatti mediante l'esibizione di un documento di riconoscimento; **(R)**
- c) la richiesta e la produzione, da parte rispettivamente degli ufficiali di stato civile e dei direttori sanitari, del certificato di assistenza al parto ai fini della formazione dell'atto di nascita. **(R)**

Articolo 75 (R)

Decadenza dai benefici

1. Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'articolo 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante

decade dai benefici eventualmente conseguenti al provvedimento emanato sulla base della dichiarazione non veritiera.

Articolo 76 (L)

Norme penali

1. Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico è punito ai sensi del codice penale e delle leggi speciali in materia.

2. L'esibizione di un atto contenente dati non più rispondenti a verità equivale ad uso di atto falso.

3. Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'articolo 4, comma 2, sono considerate come fatte a pubblico ufficiale.

4. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte.

CAPO VII

DISPOSIZIONI FINALI

Articolo 77 (L-R)

Norme abrogate

1. Dalla data di entrata in vigore del presente testo unico sono abrogati: la legge 4 gennaio 1968 n.15; l'articolo 2, comma 15, primo periodo della legge 24 dicembre 1993 n.537; l'articolo 2 commi 3, 4, 7, 9 e 10 e l'articolo 3 commi 1, 4, 5, e 11 come sostituito dall'articolo 2, comma 10 della legge 16 giugno 1998, n. 191, della legge 15 maggio 1997 n. 127; l'articolo 2, comma 11 della citata legge 16 giugno 1998 n. 191; gli articoli 2 e 3 della legge 24 novembre 2000, n.340; l'articolo 55, comma 3 della legge 21 novembre 2000, n.342. (L)

2. Sono altresì abrogati: il D.P.R. 10 novembre 1997 n. 513; il D.P.R. 20 ottobre 1998 n. 403; il D.P.R. 20 ottobre 1998, n. 428; i commi 2 e 3 dell'articolo 37 del D.P.R. 30 maggio 1989, n. 223. **(R)**

Articolo 78 (L-R)

Norme che rimangono in vigore

1. Dalla data di entrata in vigore del presente testo unico restano comunque in vigore :

- a) le vigenti disposizioni legislative e regolamentari in materia di trasmissione delle dichiarazioni fiscali di cui al D.P.R. 22 luglio 1998, n.322, al D.P.R. 14 ottobre 1999, n.542, al D.P.R. 10 marzo 2000, n.100, al decreto direttoriale 31 luglio 1998, al decreto direttoriale 29 marzo 2000, al D.M.31 maggio 1999, n.164, e le disposizioni di cui al decreto legislativo 31 marzo 1998, n. 109 concernenti la dichiarazione sostitutiva unica per la determinazione dell'indicatore della situazione economica equivalente dei soggetti che richiedono prestazioni sociali agevolate;
- b) il D.P.R.26 ottobre 1972 n.642 in materia di imposta di bollo;
- c) gli articoli 18 e 30 della legge 7 agosto 1990 n. 241;
- d) l'articolo 2, comma 15, secondo periodo della legge 24 dicembre 1993 n.537;
- e) le disposizioni in materia di dati personali di cui alla legge 31 dicembre 1996, n. 675 e ai decreti legislativi adottati in attuazione delle leggi 31 dicembre 1996, n. 676 e 6 ottobre 1998, n. 344;
- f) fino alla loro sostituzione, i regolamenti ministeriali, le direttive e i decreti ministeriali a contenuto generale, nonché le regole tecniche già emanate alla data di entrata in vigore del presente testo unico;
- g) tutte le disposizioni legislative in materia di conservazione di beni archivistici di cui al capo II del d.Lgs. 29 ottobre 1999, n. 490.

2. Per le forze di polizia, restano in vigore, con riferimento agli articoli 43, comma 4, 59 e 60, le particolari disposizioni di legge e di regolamento concernenti i trattamenti di dati personali da parte delle forze dell'ordine, ai sensi dell'articolo 4 legge 31 dicembre 1996, n. 675.

INDICE

CAPO I Definizioni e ambito di applicazione

Art. 1 Definizioni

Art. 2 Oggetto

Art. 3 Soggetti

Art. 4 Impedimento alla sottoscrizione e alla dichiarazione

Art. 5 Rappresentanza legale

CAPO II Documentazione amministrativa

SEZIONE I Documenti amministrativi e atti pubblici

Art. 6 Riproduzione di documenti

Art. 7 Redazione e stesura di atti pubblici

SEZIONE II Documento informatico

Art. 8 Documento informatico

Art. 9 Documenti informatici delle pubbliche amministrazioni

Art. 10 Forma ed efficacia del documento informatico

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

Art. 12 Pagamenti informatici

Art. 13 Libri e scritture

SEZIONE III Trasmissione di documenti

Art. 14 Trasmissione del documento informatico

Art. 15 Trasmissione dall'estero di atti agli uffici di stato civile

Art. 16 Riservatezza dei dati personali contenuti nei documenti trasmessi

Art. 17 Segretezza della corrispondenza trasmessa per via telematica

SEZIONE IV Copie autentiche, autenticazione di sottoscrizioni

Art. 18 Copie autentiche

Art. 19 Modalità alternative all'autenticazione di copie

Art. 20 Copie di atti e documenti informatici

Art. 21 Autenticazione delle sottoscrizioni

SEZIONE V Firma digitale

Art. 22 Definizioni

Art. 23 Firma digitale

Art. 24 Firma digitale autenticata

Art. 25 Firma di documenti informatici delle pubbliche amministrazioni

Art. 26 Deposito della chiave privata

Art. 27 Certificazione delle chiavi

Art. 28 Obblighi dell'utente e del certificatore

Art. 29 Chiavi di cifratura della pubblica amministrazione

SEZIONE VI Legalizzazione di firme e di fotografie

Art. 30 Modalità per la legalizzazione di firme

Art. 31 Atti non soggetti a legalizzazione

Art. 32 Legalizzazione di firme di capi di scuole parificate o legalmente riconosciute

Art. 33 Legalizzazione di firme di atti da e per l'estero

Art. 34 Legalizzazione di fotografie

SEZIONE VII Documenti di riconoscimento e di identità

Art. 35 Documenti di identità e di riconoscimento

Art. 36 Carta di identità e documenti elettronici

SEZIONE VIII Regime fiscale

Art. 37 Esenzioni fiscali

CAPO III Semplificazione della documentazione amministrativa

SEZIONE I Istanze e dichiarazioni da presentare alla pubblica amministrazione

Art. 38 Modalità di invio e sottoscrizione delle istanze

Art. 39 Domande per la partecipazione a concorsi pubblici

SEZIONE II Certificati

Art. 40 Certificazioni contestuali

Art. 41 Validità dei certificati

Art. 42 Certificati di abilitazione

SEZIONE III Acquisizione diretta di documenti

Art. 43 Accertamenti d'ufficio

Art. 44 Acquisizione di estratti degli atti dello stato civile

SEZIONE IV Esibizione di documento

Art. 45 Documentazione mediante esibizione

SEZIONE V Norme in materia di dichiarazioni sostitutive

Art. 46 Dichiarazioni sostitutive di certificazioni

Art. 47 Dichiarazioni sostitutive dell'atto di notorietà

Art. 48 Disposizioni generali in materia di dichiarazioni sostitutive

Art. 49 Limiti di utilizzo delle misure di semplificazione

CAPO IV Sistema di gestione informatica dei documenti

SEZIONE I Disposizioni sulla gestione informatica dei documenti

Art. 50 Attuazione dei sistemi

Art. 51 Sviluppo dei sistemi informativi delle pubbliche amministrazioni

Art. 52 Il sistema di gestione informatica dei documenti

Art. 53 Registrazione di protocollo

Art. 54 Informazioni annullate o modificate

Art. 55 Segnatura di protocollo

Art. 56 Operazioni ed informazioni minime del sistema di gestione

informatica dei documenti

Art. 57 Numero di protocollo

SEZIONE II Accesso ai documenti e alle informazioni del sistema

Art. 58 Funzioni di accesso ai documenti e alle informazioni del sistema

Art. 59 Accesso esterno

Art. 60 Accesso effettuato dalle pubbliche amministrazioni

SEZIONE III Tenuta e conservazione del sistema di gestione dei documenti

Art. 61 Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi

Art. 62 Procedure di salvataggio e conservazione delle informazioni del sistema

Art. 63 Registro di emergenza

SEZIONE IV Sistema di gestione dei flussi documentali

Art. 64 Sistema di gestione dei flussi documentali

Art. 65 Requisiti del sistema per la gestione dei flussi documentali

Art. 66 Specificazione delle informazioni previste dal sistema di gestione dei flussi documentali

SEZIONE V Disposizioni sugli archivi

Art. 67 Trasferimento dei documenti all'archivio di deposito

Art. 68 Disposizioni per la conservazione degli archivi

Art. 69 Archivi storici

SEZIONE VI Attuazione ed aggiornamento dei sistemi

Art. 70 Aggiornamenti del sistema

CAPO V Controlli

	Art.	71
Modalità dei controlli		
	Art.	72
Responsabilità dei controlli		
	CAPO	VI

Sanzioni

	Art.	73
Assenza di responsabilità della pubblica amministrazione		
	Art.	74
Violazione dei doveri d'ufficio		
	Art.	75
Decadenza dai benefici		
	Art.	76
Norme penali		

CAPO VII Disposizioni finali

Art.

77 Norme abrogate

Art. 78

Norme che rimangono in vigore

**TAVOLA DI CORRISPONDENZA
DEI RIFERIMENTI PREVIGENTI AL
TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E
REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE
AMMINISTRATIVA**

ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
Articolo 1 (<i>Definizioni</i>) comma 1 lettera a)	articolo 22, comma 2 L.241/90 e art. 7, comma 6 D.P.R. 403/98
comma 1 lettera b)	articolo 1, comma 1, lett. a) D.P.R. 513/97
comma 1 lettere c), d)	----
comma 1 lettera e)	articolo1, comma1, lett.b) D.P.C.M. n. 437/99
comma 1 lettere f), g), h)	----
comma 1 lettera i)	articolo 20, secondo comma L.15/68
comma 1 lettera l)	articolo 15, primo comma L.15/68
comma 1 lettera m)	----
comma 1 lettera n)	articolo 1, comma 1 lett. b) D.P.R. 513/97
comma 1 lettere o), p)	----
comma 1 lettera q), primo periodo	articolo 1 D.P.R. 428/98
comma 1 lettera q), secondo periodo	articolo 2, comma 1 D.P.R. 428/98
comma 1 lettera r)	articolo 1 D.P.R. 428/98
comma 1 lettera s)	articolo 1 D.P.R. 428/98
Articolo 2 (<i>Oggetto</i>) comma 1	articolo 1 L.15/68 e articolo 2 comma 1, primo periodo L.340/2000
Articolo 3 (<i>Soggetti</i>) comma 1	articolo 5, comma 1 D.P.R. 403/98
comma 2	articolo 5, comma 2 D.P.R. 403/98
comma 3	----
comma 4	articolo 2 comma 2 D.P.R. 394/99
Articolo 4 (<i>Impedimento alla sottoscrizione e alla dichiarazione</i>) comma 1	articolo 4 D.P.R. 403/98
comma 2	----
comma 3	----
Articolo 5 (<i>Rappresentanza legale</i>) comma 1	articolo 8 L.15/68
Articolo 6 (<i>Riproduzione e conservazione di documenti</i>) comma 1	articolo 25 L.15/68 e art.15 D.P.R. 513/1997
comma 2	articolo 2, comma 15, primo periodo L.537/1993
comma 3	----

comma 4	----
Articolo 7 (<i>Redazione e stesura di atti pubblici</i>) comma 1	articolo 12, primo comma L.15/68
comma 2	articolo 13 primo e secondo comma L.15/68
Articolo 8 (<i>Documento informatico</i>) comma 1	articolo 2 D.P.R. 513/97
comma 2	articolo 3, comma 1 e 2 D.P.R. 513/97
comma 3	articolo 3, comma 3 D.P.R. 513/97
comma 4	articolo 3, comma 4 D.P.R. 513/97
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
Articolo 9 (<i>Documenti informatici delle pubbliche amministrazioni</i>) comma 1	articolo 18, comma 1 D.P.R. 513/97
comma 2	articolo 18, comma 2 D.P.R. 513/97
comma 3	articolo 22, comma 1 D.P.R. 513/97
comma 4	articolo 18 comma 3 D.P.R. 513/97
Articolo 10 (<i>Forma ed efficacia del documento informatico</i>) comma 1	articolo 4, comma 1 D.P.R. 513/97
comma 2	articolo 4, comma 2 D.P.R. 513/97
comma 3	articolo 5, comma 1 D.P.R. 513/97
comma 4	articolo 5, comma 2 D.P.R. 513/97
Articolo 11 (<i>Contratti stipulati con strumenti informatici o per via telematica</i>) comma 1	articolo 11, comma 1 D.P.R. 513/97
comma 2	articolo 11, comma 2 D.P.R. 513/97
Articolo 12 (<i>Pagamenti informatici</i>) comma 1	articolo 14 D.P.R. 513/97
Articolo 13 (<i>Libri e scritture</i>) comma 1	articolo 15 D.P.R. 513/97
Articolo 14 (<i>Trasmissione del documento informatico</i>) comma 1	articolo 12, comma 1 D.P.R. 513/97
comma 2	articolo 12, comma 2 D.P.R. 513/97
comma 3	articolo 12, comma 3 D.P.R. 513/97

Articolo 15 (<i>Trasmissione dall'estero di atti agli uffici di stato civile</i>) comma 1	articolo 19 L.15/68
Articolo 16 (<i>Riservatezza dei dati personali contenuti nei documenti trasmessi</i>) comma 1	articolo 8, comma 1 D.P.R. 403/98
comma 2	articolo 8, comma 2 D.P.R. 403/98
comma 3	articolo 8, comma 2 D.P.R. 403/98
Articolo 17 (<i>Segretezza della corrispondenza trasmessa per via telematica</i>) comma 1	articolo 13, comma 1 D.P.R. 513/97
comma 2	articolo 13, comma 2 D.P.R. 513/97
Articolo 18 (<i>Copie autentiche</i>) comma 1	articolo 14, primo comma e articolo 7, primo comma L.15/68
comma 2	articolo 14, secondo comma L.15/68
comma 3	articolo 3, comma 4 D.P.R. 403 /98
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
Articolo 19 (<i>Modalità alternative all'autenticazione di copie</i>) comma 1	articolo 2, comma 2 D.P.R. 403/98
Articolo 20 (<i>Copie di atti e documenti informatici</i>) comma 1	articolo 6, comma 1 D.P.R. 513/97
comma 2	articolo 6, comma 2 D.P.R. 513/97
comma 3	articolo 6, comma 3 D.P.R. 513/97
comma 4	articolo 6, comma 4 D.P.R. 513/97
comma 5	articolo 6, comma 5 D.P.R. 513/97
Articolo 21 (<i>Autenticazione delle sottoscrizioni</i>) comma 1	----
comma 2	----
Articolo 22 (<i>Definizioni</i>) comma 1, lettera a)	articolo 1, comma 1 lett. c) D.P.R. 513/97
comma 1, lettera b)	articolo 1, comma 1 lett. d) D.P.R. 513/97
comma 1, lettera c)	articolo 1, comma 1 lett. e) D.P.R.

	513/97
comma 1, lettera d)	articolo 1, comma 1 lett. f) D.P.R. 513/97
comma 1, lettera e)	articolo 1, comma 1 lett. g) D.P.R. 513/97
comma 1, lettera f)	articolo 1, comma 1 lett. h) D.P.R. 513/97
comma 1, lettera g)	articolo 1, comma 1 lett. i) D.P.R. 513/97
comma 1, lettera h)	articolo 1, comma 1 lett. l) D.P.R. 513/97
comma 1, lettera i)	articolo 1, comma 1 lett. m) D.P.R. 513/97
comma 1, lettera l)	articolo 1, comma 1 lett. n) D.P.R. 513/97
comma 1, lettera m)	articolo 1, comma 1 lett. o) D.P.R. 513/97
comma 1, lettera n)	articolo 1, comma 1 lett. p) D.P.R. 513/97
comma 1, lettera o)	articolo 1, comma 1 lett. q) D.P.R. 513/97
Articolo 23 (<i>Firma digitale</i>)	
comma 1	articolo 10, comma 1 D.P.R. 513/97
comma 2	articolo 10, comma 2 D.P.R. 513/97
comma 3	articolo 10, comma 3 D.P.R. 513/97
comma 4	articolo 10, comma 4 D.P.R. 513/97
comma 5	articolo 10, comma 5 D.P.R. 513/97
comma 6	articolo 10, comma 6 D.P.R. 513/97
comma 7	articolo 10, comma 7 D.P.R. 513/97
Articolo 24 (<i>Firma digitale autenticata</i>)	
comma 1	articolo 16, comma 1 D.P.R. 513/97
comma 2	articolo 16, comma 2 D.P.R. 513/97
comma 3	articolo 16, comma 3 D.P.R. 513/97
comma 4	articolo 16, comma 4 D.P.R. 513/97
comma 5	articolo 16, comma 5 D.P.R. 513/97
comma 6	articolo 16, comma 6 D.P.R. 513/97
Articolo 25 (<i>Firma di documenti informatici delle pubbliche amministrazioni</i>)	
comma 1	articolo 19, comma 1 D.P.R. 513/97
comma 2	articolo 19, comma 2 D.P.R. 513/97
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE

Articolo 26 (<i>Deposito della chiave privata</i>) comma 1	articolo 7, comma 1 D.P.R. 513/97
comma 2	articolo 7, comma 2 D.P.R. 513/97
comma 3	articolo 7, comma 3 D.P.R. 513/97
Articolo 27 (<i>Certificazione delle chiavi</i>) comma 1	articolo 8, comma 1 D.P.R. 513/97
comma 2	articolo 8, comma 2 D.P.R. 513/97
comma 3	articolo 8, comma 3 D.P.R. 513/97
comma 4	articolo 8, comma 4 D.P.R. 513/97
Articolo 28 (<i>Obblighi dell'utente e del certificatore</i>) comma 1	articolo 9, comma 1 D.P.R. 513/97
comma 2	articolo 9, comma 2 D.P.R. 513/97
Articolo 29 (<i>Chiavi di cifratura della pubblica amministrazione</i>) comma 1	articolo 17, comma 1 D.P.R. 513/97
comma 2	articolo 17, comma 2 D.P.R. 513/97
comma 3	articolo 17, comma 3 D.P.R. 513/97
comma 4	articolo 17, comma 4 D.P.R. 513/97
Articolo 30 (<i>Modalità per la legalizzazione di firme</i>) comma 1	articolo 15 secondo comma L.15/68
Articolo 31 (<i>Atti non soggetti a legalizzazione</i>) comma 1	articolo 18, primo e secondo comma L.15/68
Articolo 32 (<i>Legalizzazione di firme di capi di scuole parificate o legalmente riconosciute</i>) comma 1	articolo 16 L.15/68
Articolo 33 (<i>Legalizzazione di firme di atti da e per l'estero</i>) comma 1	articolo 17, primo comma L.15/68
comma 2	articolo 17, secondo comma L.15/68
comma 3	articolo 17, terzo comma L.15/68
comma 4	articolo 17, quarto comma L.15/68
comma 5	articolo 17, quinto comma L.15/68
Articolo 34 (<i>Legalizzazione di fotografie</i>) comma 1	articolo 2, comma 7 L.127/97 come modificato dall'articolo 55 comma 3 della L.342/2000
Articolo 35 (<i>Documenti di identità e di riconoscimento</i>) comma 1	----
comma 2	articolo 292 R.D. n. 635/40
comma 3	articolo 2, comma 9 L.127/97

Articolo 36 (<i>Carta d'identità e documenti elettronici</i>) comma 1	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
comma 2	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
comma 3	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
comma 4	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
comma 5	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
comma 6	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
comma 7	articolo 2, comma 10 L.127/97 come modificato dall'articolo 2, comma 4 L.191/98
Articolo 37 (<i>Esenzioni fiscali</i>) comma 1	articolo 21, primo comma L.15/68
comma 2	articolo 23, primo comma L.15/68
Articolo 38 (<i>Modalità di invio e sottoscrizione delle istanze</i>) comma 1	art.3 comma 11 della L.127/97 come modificato dall'art. 2 comma 10 della L.191/98
comma 2	----
comma 3	articolo 3, comma 11 L.127/97, come modificato dall'art.2 comma 10 della L.191/98
Articolo 39 (<i>Domande per la partecipazione a concorsi pubblici</i>) comma 1	articolo 3, comma 5 L.127/97
Articolo 40 (<i>Certificazioni contestuali</i>) comma 1	articolo 11 L.15/68
Articolo 41 (<i>Validità dei certificati</i>) comma 1	articolo 2, comma 3 L.127/97, come modificato dall'art.2 comma 2 della L.191/98
comma 2	articolo 2, comma 4 L.127/97

Articolo 42 (<i>Certificati di abilitazione</i>) comma 1	articolo 12 D.P.R. 403/98
Articolo 43 (<i>Accertamenti d'ufficio</i>) comma 1	----
comma 2	articolo 3, comma 1 L.340/2000
comma 3	----
comma 4	----
comma 5	articolo 7, comma 2 D.P.R. 403/98
comma 6	articolo 7, comma 3 D.P.R. 403/98
Articolo 44 (<i>Acquisizione di estratti degli atti dello stato civile</i>) comma 1	articolo 9, comma 1 D.P.R. 403/98
comma 2	articolo 9, comma 2 D.P.R. 403/98
Articolo 45 (<i>Documentazione mediante esibizione</i>) comma 1	articolo 3, comma 1 L.127/97
comma 2	articolo 7, comma 4 D.P.R. 403/98
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
comma 3	----
Articolo 46 (<i>Dichiarazioni sostitutive di certificazioni</i>) comma 1	articolo 2, primo comma L.15/68 e articolo 1, comma 1 D.P.R. 403/1998
Articolo 47 (<i>Dichiarazioni sostitutive dell'atto di notorietà</i>) comma 1	articolo 4, primo comma L.15/68
comma 2	articolo 2, comma 2 D.P.R. 403/98
comma 3	articolo 2, comma 1 D.P.R. 403/98
comma 4	----
Articolo 48 (<i>Disposizioni generali in materia di dichiarazioni sostitutive</i>) comma 1	articolo 6, comma 1 D.P.R. 403/98
comma 2	articolo 6, comma 2 D.P.R. 403/98
comma 3	articolo 6, comma 3 D.P.R. 403/98
Articolo 49 (<i>Limiti di utilizzo delle misure di semplificazione</i>) comma 1	articolo 10, comma 1 D.P.R. 403/98
comma 2	articolo 10, comma 2 D.P.R. 403/98
Articolo 50 (<i>Attuazione dei sistemi</i>) comma 1	articolo 21, comma 1 D.P.R. 428/98

comma 2	articolo 21, comma 2 D.P.R. 428/98
comma 3	articolo 21, comma 3 D.P.R.428/98
comma 4	articolo 2, comma 2 D.P.R.428/98
comma 5	articolo 2, comma 3 D.P.R. 428/98
Articolo 51 (<i>Sviluppo dei sistemi informativi delle pubbliche amministrazioni</i>) comma 1	articolo 20, comma 1 D.P.R. 513/97
comma 2	articolo 20, comma 2 D.P.R. 513/97
comma 3	articolo 20, comma 3 D.P.R. 513/97
Articolo 52 (<i>Sistema di gestione informatica dei documenti</i>) comma 1	articolo 3 D.P.R. 428/98
Articolo 53 (<i>Registrazione di protocollo</i>) comma 1	articolo 4, comma 1 D.P.R. 428/98
comma 2	articolo 4, comma 2 D.P.R. 428/98
comma 3	articolo 4, comma 3 D.P.R. 428/98
comma 4	articolo 4, comma 4 D.P.R. 428/98
comma 5	articolo 4, comma 5 D.P.R. 428/98
Articolo 54 (<i>Informazioni annullate o modificate</i>) comma 1	articolo 5 comma 1 e comma 2 D.P.R. 428/98
comma 2	articolo 5 comma 1 D.P.R. 428/98
Articolo 55 (<i>Segnatura di protocollo</i>) comma 1	articolo 6, comma 1 D.P.R. 428/98
comma 2	articolo 6, comma 2 D.P.R. 428/98
comma 3	articolo 6, comma 3 D.P.R. 428/98
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
comma 4	articolo 6, comma 4 D.P.R. 428/98
comma 5	articolo 6, comma 5 D.P.R. 428/98
Articolo 56 (<i>Informazioni minime del sistema di gestione informatica dei documenti</i>) comma 1	articolo 7 D.P.R. 428/98
Articolo 57 (<i>Numero di protocollo</i>) comma 2	articolo 8 D.P.R. 428/98
Articolo 58 (<i>Funzioni di accesso ai documenti e alle informazioni del sistema</i>) comma 1	articolo 9, comma 1 D.P.R. 428/98
comma 2	articolo 9, comma 2 D.P.R. 428/98
comma 3	articolo 9, comma 3 D.P.R. 428/98
Articolo 59 (<i>Accesso esterno</i>)	

comma 1	articolo 10, comma 1 D.P.R. 428/98
comma 2	articolo 10, comma 2 D.P.R. 428/98
comma 3	articolo 10, comma 3 D.P.R. 428/98
comma 4	articolo 10, comma 4 D.P.R. 428/98
Articolo 60 (<i>Accesso effettuato dalle pubbliche amministrazioni</i>) comma 1	articolo 11, comma 1 D.P.R. 428/98
comma 2	articolo 11, comma 2 D.P.R. 428/98
comma 3	articolo 11, comma 4 D.P.R. 428/98
Articolo 61 (<i>Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi</i>) comma 1	articolo 12, comma 1 D.P.R. 428/98
comma 2	articolo 12, comma 2 D.P.R. 428/98
comma 3	articolo 12, comma 3 D.P.R. 428/98
Articolo 62 (<i>Procedure di salvataggio e conservazione delle informazioni del sistema</i>) comma 1	articolo 13, comma 1 D.P.R. 428/98
comma 2	articolo 13, comma 2 D.P.R. 428/98
comma 3	articolo 13, comma 3 D.P.R. 428/98
comma 4	articolo 13, comma 4 D.P.R. 428/98
Articolo 63 (<i>Registro di emergenza</i>) comma 1	articolo 14, comma 1 D.P.R. 428/98
comma 2	articolo 14, comma 2 D.P.R. 428/98
comma 3	articolo 14, comma 3 D.P.R. 428/98
comma 4	articolo 14, comma 4 D.P.R. 428/98
comma 5	articolo 14, comma 5 D.P.R. 428/98
Articolo 64 (<i>Sistema di gestione dei flussi documentali</i>) comma 1	articolo 15, comma 2 D.P.R. 428/98
comma 2	articolo 15, comma 1 D.P.R. 428/98
comma 3	articolo 15, comma 3 D.P.R. 428/98
comma 4	articolo 15, comma 4 D.P.R. 428/98
ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
Articolo 65 (<i>Requisiti del sistema per la gestione dei flussi documentali</i>) comma 1	articolo 16 D.P.R. 428/98
Articolo 66 (<i>Specificazione delle informazioni previste dal sistema di gestione dei flussi</i>)	

<i>sistema di gestione dei flussi documentali</i> comma 1	articolo 17 D.P.R. 428/98
Articolo 67 (<i>Trasferimento dei documenti all'archivio di deposito</i>) comma 1	articolo 18, comma 1 D.P.R. 428/98
comma 2	articolo 18, comma 2 D.P.R. 428/98
comma 3	----
Articolo 68 (<i>Disposizioni per la conservazione degli archivi</i>) comma 1	articolo 19, comma 1 D.P.R. 428/98
comma 2	articolo 19, comma 2 D.P.R. 428/98
comma 3	articolo 19, comma 3 D.P.R. 428/98
Articolo 69 (<i>Archivi storici</i>) comma 1	articolo 20 D.P.R. 428/98
Articolo 70 (<i>Aggiornamenti del sistema</i>) comma 1	articolo 22 D.P.R. 428/98
Articolo 71 (<i>Modalità dei controlli</i>) comma 1	articolo 11, comma 1 D.P.R. 403/98
comma 2	articolo 11, comma 2 D.P.R. 403/98
comma 3	----
comma 4	articolo 2 comma 1, secondo periodo L.340/2000
Articolo 72 (<i>Responsabilità dei controlli</i>) comma 1	----
comma 2	----
Articolo 73 (<i>Assenza di responsabilità della pubblica amministrazione</i>) comma 1	articolo 24 L.15/68
Articolo 74 (<i>Violazione dei doveri d'ufficio</i>) comma 1	articolo 3, comma 4 L.127/97
comma 2, lettera a)	articolo 3, comma 3 D.P.R.403/98
comma 2, lettera b)	articolo 7, comma 5 D.P.R.403/98
comma 2, lettera c)	----
Articolo 75 (<i>Decadenza dai benefici</i>) comma 1	articolo 11, comma 3 D.P.R.403/98
Articolo 76 (<i>Norme penali</i>) comma 1	articolo 26, primo comma L.15/68
comma 2	articolo 26, secondo comma L.15/68
comma 3	articolo 26, secondo comma L.15/68
comma 4	articolo 26, terzo comma L.15/68
Articolo 77 (<i>Norme abrogate</i>) comma 1	----

ARTICOLATO DEL TESTO UNICO	RIFERIMENTO PREVIGENTE
comma 2	----
Articolo 78 (<i>Norme che rimangono in vigore</i>) comma 1	----

APPENDICE

PROVVEDIMENTI CONTENENTI LE REGOLE TECNICHE, CHE, IN BASE ALL'ART. 78, COMMA 1, LETT. D) DELLO SCHEMA DI TESTO UNICO, RESTANO IN VIGORE:

1. D.P.C.M. 11 settembre 1974 “Norme per la fotoreproduzione sostitutiva dei documenti di archivio e di altri atti delle pubbliche amministrazioni”;
2. D.P.C.M. 6 dicembre 1996, n. 694 “Regolamento recante norme per la riproduzione sostitutiva dei documenti di archivio e di altri atti dei privati”;
3. deliberazione AIPA n. del 9 novembre 1995, recante: “Definizione delle regole tecniche per il mandato informatico”, in G.U. n. 273 del 22 novembre 1995;
4. deliberazione AIPA n. del 30 luglio 1998, recante: “Regole tecniche per l'uso di supporti ottici (art. 2, comma 15, della legge 24 dicembre 1993, n. 537)”, in G.U. n. 192 del 19 agosto 1998;
5. D.P.C.M. 8 febbraio 1999, recante: “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. 10 novembre 1997, n. 513”, in G.U. n. 87 del 15 aprile 1999;
6. circolare AIPA n. 22 del 26 luglio 1999, recante: “Art. 16, comma 1, dell'allegato tecnico del d.P.C.M. 8 febbraio 1999 – Modalità per presentare domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'art. 8, comma 3, del d.P.R. 10 novembre 1997, n. 513”, in G.U. n.179 del 2 agosto 1999;
7. D.P.C.M. 22 ottobre 1999, n.437, recante: “Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento d'identità elettronica, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n.127, come modificato dall'articolo 2, comma 4, dalla legge 16 giugno 1998, n.191.”, in G.U. n.277 del 25 novembre 1999;
8. circolare AIPA n.24 del 19 giugno 2000, recante: “Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.”, in G.U. n. 151 del 30 giugno 2000;
9. decreto del Ministero dell'interno 19 luglio 2000, recante: “Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.”, in Supplemento ordinario n.116 alla G.U. n.169 del 21 luglio 2000;
10. D.P.C.M. 31 ottobre 2000, recante: “Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n.428.”, in G.U. n.272 del 21 novembre 2000;

11. deliberazione AIPA n. 51/2000 del 23 novembre 2000, recante: "Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del d.P.R. 10 novembre 1997, n. 513", in corso di pubblicazione.

D.P.C.M. 11 settembre 1974

Norme per la fotoreproduzione sostitutiva dei documenti di archivio e di altri atti delle pubbliche amministrazioni



IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'art. 25 della legge 4 gennaio 1968, n. 15;

Udita la commissione di cui all'art. 12 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409;

Sentiti i Ministri per l'interno, per la grazia e giustizia, per le finanze e per il tesoro;

Decreta:

1. Limiti, modalità e procedimenti tecnici per la fotoreproduzione sostitutiva.

La facoltà di riproduzione fotografica sostitutiva di documenti di archivio e di altri atti delle pubbliche amministrazioni, compresi gli enti pubblici economici, prevista dall'art. 25 della legge 4 gennaio 1968, n. 15, può essere esercitata nei limiti, con le modalità ed i procedimenti tecnici stabiliti dal presente decreto.

2. Atti e documenti per i quali è ammessa la fotoreproduzione sostitutiva.

La facoltà di riproduzione fotografica sostitutiva, prevista dall'art. 25 della legge 4 gennaio 1968, n. 15, non può essere esercitata per gli atti e documenti compresi nelle categorie sotto specificate:

- a) raccolte e documenti singoli per i quali sia stato adottato dalle competenti autorità il provvedimento di riconoscimento di interesse particolarmente importante o di notevole interesse storico ai sensi delle vigenti disposizioni;
- b) leggi, atti aventi forza di legge, decreti inseriti nelle raccolte ufficiali, regolamenti esterni, statuti degli enti pubblici;
- c) sentenze della Corte costituzionale;
- d) trattati internazionali ed atti connessi;
- e) piani regolatori generali e particolari; piani di fabbricazione, di lottizzazione, per l'industrializzazione ed analoghi;
- f) fascicoli personali e stati matricolari dei dipendenti dello Stato e delle altre pubbliche amministrazioni, in attività di servizio;
- g) registro generale d'ordine delle conservatorie delle ipoteche, pubblico registro automobilistico, pubblico registro navale, registro ed originali degli atti dello stato civile da conservare presso i comuni e tutti gli altri registri prescritti dalla legge come mezzo per la pubblicità dei fatti giuridici;
- h) originali dei contratti per importo superiore ai settantacinque milioni, redatti in forma pubblica amministrativa o per scrittura privata autenticata;
- i) originali degli atti formati e conservati dai notai e dalle persone autorizzate a esercitare le funzioni di notaio ai sensi dell'art. 6 della legge 16 febbraio 1913, n. 89, ed i testamenti olografici consegnati fiduciarmente agli stessi, anche successivamente al loro versamento agli archivi notarili;
- l) originali degli atti ricevuti dai capi degli archivi notarili e annotati al prescritto repertorio, comprese le copie degli atti notarili rogati in paese estero; gli originali e le copie delle scritture private che gli uffici del registro, ai sensi dell'art. 17 del decreto del Presidente della Repubblica 26 ottobre 1972, n. 634, trasmettono agli archivi notarili;
- m) atti contenenti disegni e scritture originali in cui la colorazione abbia un particolare significato;
- n) libri-giornali, degli inventari sociali e fiscali obbligatori concernenti le attività imprenditoriali;
- o) diplomi originali attestanti gli studi compiuti, rilasciati nelle scuole di ogni ordine e grado.

Per le sentenze, le decisioni e gli altri provvedimenti giurisdizionali dei giudici ordinari e delle giurisdizioni speciali, e relativi fascicoli d'ufficio, la citata facoltà di fotoreproduzione non può essere esercitata prima di 10 anni dal passaggio in giudicato o dalla irrevocabilità della sentenza o decisione.

3. Adempimenti preliminari all'esercizio delle facoltà di fotoreproduzione sostitutiva.

Le pubbliche amministrazioni che intendano avvalersi della facoltà di cui all'art. 25 della legge 4 gennaio 1968, n. 15, devono inoltrare al Ministero dell'interno - Direzione generale degli archivi di Stato, una relazione sulle categorie di atti e documenti, compresi nei massimari di scarto anche per settori di servizio, che intendono sostituire con la riproduzione fotografica. La relazione deve indicare dati riguardanti la determinazione delle serie archivistiche, il sistema di riproduzione, quello adottato per la cartellinatura e le caratteristiche delle eventuali copie da utilizzarsi per gli usi correnti e di consultazione. Alla relazione medesima devono essere allegati i fac-simile degli schemi di cartellinatura e dei mezzi di consultazione previsti per la ricerca dei singoli documenti o delle unità archivistiche, nonché prove positive e negative a seconda delle caratteristiche intrinseche e morfologiche presentate dagli originali cartacei.

La relazione e le prove sono sottoposte al parere della commissione per la fotoreproduzione dei documenti di cui all'art. 12 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, ai fini della emanazione del decreto del Ministro per l'interno previsto al terzo comma del citato art. 25 della legge 4 gennaio 1968, numero 15. Si considera acquisito il parere favorevole della commissione trascorso un semestre dalla richiesta dell'amministrazione interessata.

Le stesse procedure devono essere osservate per ogni ulteriore categoria di atti e documenti d'archivio che si intenda sostituire con la fotoreproduzione.

4. Distruzione dei documenti fotoreprodotti.

Le pubbliche amministrazioni possono procedere alla distruzione degli atti e documenti conservati, di cui è stata effettuata la fotoreproduzione sostitutiva, soltanto se riferentisi ad un periodo anteriore all'ultimo triennio. Qualora regolamenti o norme particolari dovessero prevedere per alcune serie un periodo limitato di validità o di conservazione nel tempo, queste, effettuata la fotoreproduzione sostitutiva, possono essere distrutte dopo un terzo di tale periodo. I bollettini di versamento in conto corrente postale ed i titoli dei servizi a denaro dell'Amministrazione delle poste e delle telecomunicazioni, una volta effettuata la fotoreproduzione sostitutiva, non sono soggetti all'obbligo della conservazione.

I registri ed i libri comunque denominati, non esclusi dall'applicazione dell'art. 25 della legge 4 gennaio 1968, n. 15, ai sensi dell'art. 2 del presente decreto, non possono essere fotoreprodotti se non siano anche esauriti.

Alla distruzione dei documenti e degli atti fotoreprodotti può procedersi dopo effettuate le operazioni di collaudo e di autenticazione ai sensi degli articoli 8 e 9 e comunque non prima che siano decorsi 180 giorni dalla pubblicazione nella Gazzetta Ufficiale del decreto del Ministro per l'interno previsto dal terzo comma del citato art. 25.

L'Amministrazione degli archivi di Stato ha facoltà di vietare la distruzione dei documenti ed atti che la stessa ritenga opportuno ritirare e conservare a proprie spese.

5. Cartellinatura degli atti e documenti da riprodurre.

Gli atti e documenti destinati ad essere distrutti dopo la fotoreproduzione, anche se ritirati dall'Amministrazione degli archivi di Stato ai sensi dell'ultimo comma dell'art. 4 del presente decreto, devono essere cartellinati da appositi incaricati.

La cartellinatura consiste nella revisione ed opportuna preparazione degli atti e documenti da riprodurre e nell'approntamento di idonei strumenti di consultazione, eventualmente integrati da opportune codificazioni per l'elaborazione elettronica, che, in base alle indicazioni apposte sui documenti ed a quelle inserite in ciascun programma in sede tecnica di fotoreproduzione, consentano di rilevare la stretta connessione degli atti e documenti riprodotti con il loro raggruppamento (serie e unità archivistiche) e di reperire prontamente l'atto o documento da consultare o duplicare.

In particolare, salvo quanto previsto all'ultimo comma del successivo art. 7, devono essere osservate le seguenti modalità:

1) le unità archivistiche (fascicoli, registri e simili) devono essere numerate progressivamente nell'interno di ciascuna serie o raggruppamento, la cui indicazione va riportata nel frontespizio;

2) gli atti e documenti compresi in ciascuna unità archivistica devono essere ordinati e numerati, ed eventualmente codificati, progressivamente, secondo l'ordine cronologico ad iniziare dal documento meno recente, salvo che non si tratti di atti e documenti che per esigenze organizzative siano ordinati diversamente o siano già legati in volume o riportati nel registro già numerati progressivamente, per i quali resta fermo il relativo ordine;

3) le pagine di cui si compone ciascun documento compreso nell'unità archivistica, o la medesima unità archivistica se questa è composta da un unico documento, devono essere numerate progressivamente;

4) l'indicazione della serie di appartenenza di ciascun atto o documento può risultare da un titolo corrente, da un simbolo, ecc. Potrà comunque essere adottato qualsiasi sistema di individuazione purché rispondente ai criteri dettati al secondo comma del presente articolo;

5) la numerazione, che deve risultare in maniera chiara e completa, può essere effettuata manualmente o meccanicamente. Eventuali errori saranno corretti annullando l'indicazione errata e ripetendo a fianco quella esatta;

6) ciascuna unità archivistica deve essere descritta a cura dell'addetto alle operazioni di cartellinatura in un registro di serie, nel quale sono riportate le indicazioni atte ad identificarla (e cioè depositario dei documenti, numero ed estremi cronologici della serie, numero dell'unità archivistica, numero del documento e relativi estremi cronologici), la denominazione del laboratorio cui è affidata la riproduzione dei documenti, la data della riproduzione, gli estremi di classificazione delle unità fotografiche risultanti dal registro di cui al nono comma del successivo art. 7, le unità fotografiche corrispondenti a ciascuna unità archivistica, la qualifica e le generalità del pubblico ufficiale che attesta la conformità delle duplicazioni agli originali riprodotti. Per gli atti e documenti suscettibili di rettifiche, cambiamenti e successive annotazioni devono, altresì, essere riportati gli estremi relativi a tali variazioni, necessarie e sufficienti per individuare l'atto o il documento o la relativa riproduzione fotografica che le contiene; per questi ultimi nel relativo registro di serie saranno riprodotti gli estremi idonei ad individuare l'atto o documento originario cui si riferiscono. I registri di serie devono essere, prima dell'uso, numerati progressivamente per ogni pagina, e quindi vidimati da un impiegato di ruolo appositamente designato dal capo dell'ufficio responsabile della conservazione degli atti e documenti.

Qualora la documentazione da riprodurre non sia ripartita o ripartibile in serie, le unità archivistiche devono essere elencate secondo l'ordine ed i criteri indicati nella prima pagina del registro, riservato all'elencazione di tali atti e documenti.

6. Procedimenti tecnici per la riproduzione.

Il microfilm sostitutivo degli atti e documenti dei quali si intende procedere alla distruzione è costituito da un negativo soggetto alla prescrizione del presente regolamento o da altro tipo di film, che, a giudizio degli organi preposti alla normalizzazione, offra le stesse garanzie.

Per la riproduzione di documenti d'archivio ed altri atti seguita da distruzione dell'originale, ai sensi e per gli effetti dell'art. 25 della legge 4 gennaio 1968, n. 15, è ammesso l'uso di procedimenti tecnici, ivi compresa la microfilmatura in duplex, che diano garanzia di fedeltà al documento riprodotto, di duplicabilità, di leggibilità, di resistenza dell'immagine a tentativi di alterazione fraudolenta e di stabilità illimitata nel tempo, in condizioni normali di conservazione.

Quale unità fotografica può essere assunta, oltreché la bobina del tipo comunemente in commercio, qualsiasi altra pellicola negativa, di formato ridotto, di cui al primo comma del presente articolo, purché atta a costituire un complesso collegabile mediante numerazioni o altri simboli. Tali unità fotografiche, costituite da bobine o da complessi collegabili, dovranno essere numerate progressivamente e non dovranno essere impressionate sulla parte iniziale e terminale per una lunghezza di almeno dieci centimetri o, se trattasi di formati a schede, in un'unica parte per uno spazio sufficiente ai fini dell'apposizione dell'attestazione di autenticità di cui al successivo art. 9.

La pellicola da usare deve essere del tipo di sicurezza secondo gli standards internazionali di fabbricazione, da approvare con decreto del Ministro per l'interno di concerto con quelli per il tesoro e per l'industria, il commercio e l'artigianato, per l'archiviazione a tempo indeterminato, ininfiammabile, e di passo non inferiore a mm. 16. Essa può essere imperforata, monoperforata o biperforata.

Le caratteristiche di stabilità e quelle fisicochimiche devono essere attestate sugli involucri unitamente alla dicitura «pellicola di archiviazione a tempo indeterminato» ed agli estremi del relativo decreto interministeriale di approvazione.

Il trattamento della pellicola impressionata deve essere effettuato a regola d'arte.

Dal film sostitutivo, autenticato ai sensi del successivo art. 9, possono essere tratte, per le correnti esigenze operative, copie integrali o parziali. Per la formazione di tali copie sono ammessi tutti i procedimenti tecnici.

Soltanto la pellicola autenticata sostituisce, ai sensi e per gli effetti dell'art. 25 della legge 4 gennaio 1968, n. 15, gli originali atti e documenti riprodotti.

Tale pellicola deve essere custodita in modo da garantirne la leggibilità e la conservazione nel tempo. Il microfilm sostitutivo con i relativi strumenti di consultazione (di cui agli articoli 5, 6 e 7, nono comma, del presente decreto) dovrà successivamente esser versato agli archivi di Stato competenti nei termini prescritti per ciascun tipo di documentazione in essi fotoriprodotta ai sensi dell'art. 23 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409.

7. Indicazioni da apporre nel negativo sostitutivo.

La pellicola deve essere impressionata con le indicazioni sottospecificate:

- a) denominazione dell'Amministrazione o ente, tenuti a conservare gli atti e i documenti;
- b) numero o numeri di catena dell'unità fotografica, generalità complete dell'operatore alla macchina, numero della macchina e data dell'impressione;
- c) descrizione eventuale della serie (numero complessivo delle unità archivistiche ed estremi cronologici generali) data e firma del compilatore, con una nota illustrativa del contenuto e del sistema di classificazione o di numerazione usati, nonché delle eventuali dispersioni verificatesi prima della fotoriproduzione. Tali indicazioni costituiscono lo schedone generale di serie;
- d) descrizione dell'unità archivistica (numero dei documenti in essi compresi, estremi cronologici) con la denominazione completa della medesima. Tali indicazioni costituiscono lo schedone particolare dell'unità archivistica. L'eventuale mancanza di documenti, i fogli bianchi e gli eventuali danneggiamenti devono essere indicati in calce allo schedone che deve essere datato e firmato chiaramente dal compilatore. Questo schedone può essere sostituito dal frontespizio di ciascuna unità archivistica, sul quale devono essere apposte la data e la firma leggibile dell'addetto alla cartellinatura dei documenti.

Le predette indicazioni devono essere riprodotte da un quadro a caratteri mobili o da un modulo a stampa, con caratteri non inferiori al corpo 40 che ne consenta la lettura senza l'ausilio di apparecchi ottici.

Gli estremi di cui alle lettere a) e b) devono essere riprodotti all'inizio ed alla fine di ciascuna unità fotografica, come penultimo fotogramma. Su tale schedone viene apposta l'indicazione di «inizio» e di «fine» soltanto quando esso sia riprodotto prima dell'unità archivistica con la quale inizia la serie o dopo l'unità archivistica con la quale la serie termina.

Lo schedone particolare dell'unità archivistica deve essere riprodotto all'inizio e alla fine di detta unità con l'indicazione: «inizio» e «fine». Tale schedone deve altresì essere riprodotto anche quando l'unità archivistica non possa essere contenuta integralmente nella medesima unità fotografica. In tal caso saranno inserite opportune indicazioni di collegamento tra le diverse unità fotografiche riproducenti la medesima unità archivistica. Tali indicazioni saranno apposte dopo l'ultimo fotogramma riproducente l'unità archivistica in ciascuna unità fotografica ed innanzi al primo dell'unità fotografica successiva con la quale riprende la duplicazione dell'unità archivistica interrotta.

Nel caso l'unità archivistica sia costituita da un unico documento che presenti tutti gli elementi atti alla sua individuazione, può essere compilato e fotoriprodotta il solo schedone generale di serie.

I fotogrammi sono numerati progressivamente per unità fotografica e devono riprodurre gli estremi di cui al n. 4) dell'art. 5.

Ove sia essenziale lesatta ricostruzione delle dimensioni del documento, nel fotogramma deve essere riprodotta una scala centimetrica. Nei casi in cui, per necessità tecniche, sia indispensabile sezionare in più parti il documento, deve essere fotografato per ogni sezione, un quadro d'unione che, per ogni parte del documento riprodotto nel corrispondente fotogramma, presenti un quadratino nero che consenta di individuare la posizione della parte fotografata rispetto alle altre.

Le unità fotografiche devono essere descritte in apposito registro nel quale devono essere riportati gli estremi di classificazione di ciascuna e quelli idonei ad identificare le unità archivistiche in essa riprodotte secondo quanto prescritto al n. 6) dell'art. 5.

Le operazioni di ripresa e le varie fasi del trattamento devono risultare da appositi registri istituiti per ogni singola macchina, che devono essere chiusi giornalmente e sottoscritti dall'operatore.

Qualora la duplicazione sia effettuata mediante unica macchina da presa il registro prescritto al nono comma del presente articolo può fungere anche da registro di macchina. In tal caso è controfirmato dall'operatore che ha eseguito la duplicazione.

Nel caso le caratteristiche formali dei documenti non dovessero essere riconducibili al previsto sistema di cartellinatura ed alle norme tecniche prescritte, fermo restando che deve in ogni caso essere costituito un originale negativo di sicurezza per sostituire ai sensi e per gli effetti dell'art. 25 della legge 4 gennaio 1968, n. 15, i documenti riprodotti, possono essere adottate procedure la cui osservanza sia garantita da un responsabile del settore di produzione ed utilizzazione dei documenti da fotorigradare. Tale deroga è consentita anche qualora, in rapporto a strutture informative preesistenti al presente decreto, sia stato adottato un sistema di cartellinatura e di duplicazione diverso da quelli di cui agli articoli 5 e 7 da integrare con le indicazioni ricognitive principali.

8. Collaudo.

La pellicola sostitutiva dei documenti d'archivio e degli altri atti deve essere collaudata da incaricato diverso da quello che ha proceduto alla cartellinatura ed alla riproduzione fotografica.

Qualora al collaudo risultino errori di cartellinatura o di ripresa (pagine non fotografate, fotogrammi esposti in modo erroneo, fotogrammi danneggiati a seguito di incidenti verificatisi nel corso del trattamento, strappi, errori di numerazione e simili) deve provvedersi alle necessarie integrazioni e correzioni, fotografando i documenti non riprodotti o riprodotti nei fotogrammi errati o danneggiati in una o più unità fotografiche che devono avere una propria numerazione e far parte integrante della serie fotografica cui si riferiscono.

Le unità fotografiche riservate ai rifacimenti sono soggette alle modalità di registrazione e di autenticazione prescritte dal presente decreto.

All'inizio ed alla fine di ciascuna unità fotografica riservata ai rifacimenti deve risultare prima del quadro generale della riproduzione con l'indicazione dell'unità fotografica errata, uno schedone con l'indicazione rifacimenti seguita dal numero dell'unità fotografica cui le correzioni si riferiscono.

I rifacimenti sono eseguiti per ordine progressivo delle unità fotografiche in cui sono contenuti i fotogrammi da ripetere e per ciascuna unità fotografica seguendo l'ordine progressivo dei fotogrammi errati. Il numero del fotogramma da sostituire deve essere dato al rifacimento corrispondente. Il fotogramma relativo a un documento non riprodotto deve avere lo stesso numero, contrassegnato dalla lettera dell'alfabeto, del fotogramma che riproduce il documento immediatamente precedente nell'ordine di cartellinatura.

All'inizio ed alla fine del gruppo di fotogrammi che sostituiscono fotogrammi annullati della medesima unità fotografica sono riprodotte le indicazioni che contraddistinguono detta unità con la leggenda «inizio appendice» e «fine appendice»; prima e dopo i fotogrammi di ciascuna unità archivistica, ne sarà riprodotto lo schedone particolare con l'indicazione «inizio appendice» e «fine appendice».

Durante il collaudo devono essere annullati in maniera evidente ed indelebile, senza compromettere la resistenza della pellicola, tutti i fotogrammi comunque errati salvo che si tratti di duplicazioni riproducenti il medesimo documento nel qual caso si annulla il fotogramma tecnicamente peggiore.

Per quanto attiene al negativo di sostituzione, non è consentito effettuare rifacimenti complessivi che superino il cinque per cento dei fotogrammi contenuti nell'unità fotografica.

Ad operazioni ultimate il collaudatore dà atto che le riproduzioni fotografiche sono state eseguite con l'osservanza delle prescrizioni contenute nel presente decreto, mediante apposizione della propria firma sul registro di cui al nono comma del precedente art. 7, a fianco della registrazione dell'unità fotografica collaudata.

9. Autenticazione della pellicola sostitutiva.

La pellicola riprodotte gli atti e i documenti da sostituire ai sensi e per gli effetti dell'art. 25 della legge 4 gennaio 1968, n. 15, deve essere autenticata dal capo dell'ufficio responsabile della conservazione degli atti o documenti o da un suo delegato.

Il responsabile dell'autenticazione di cui al precedente comma deve assistere al procedimento di formazione della pellicola sostitutiva e, ad operazione ultimata, deve imprimere il proprio punzone sull'unità fotografica sostitutiva nelle parti non impressionate previste dall'art. 6 del presente decreto, prima che la pellicola sia sottoposta allo sviluppo. Una volta eseguito il collaudo previsto dal precedente art. 8 il funzionario autenticante applica di nuovo il punzone al termine dell'unità fotografica.

Detto punzone viene depositato, mediante impressione su apposito registro, insieme alle generalità e alla qualifica del responsabile, seguite dalle date iniziali e terminali del periodo in cui il punzone medesimo è stato usato presso l'ufficio.

Delle relative operazioni di fotoriproduzione ed autenticazione si dà atto mediante dichiarazione e firma dell'operatore che ha effettuato la ripresa e dell'incaricato dell'autenticazione sul registro di cui al nono comma del precedente art. 7, nell'apposita colonna riservata al processo verbale ed in corrispondenza dell'unità fotografica autenticata.

D.P.C.M. 6 dicembre 1996, n. 694

Regolamento recante norme per la riproduzione sostitutiva dei documenti di archivio e di altri atti dei privati.



IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'articolo 25 della legge 4 gennaio 1968, n. 15;

Visto il decreto del Presidente del Consiglio dei Ministri 11 settembre 1974 recante norme sulla fotoreproduzione sostitutiva dei documenti d'archivio e di altri atti delle pubbliche amministrazioni pubblicato nella Gazzetta Ufficiale n. 306 del 25 novembre 1974;

Vista la legge 29 gennaio 1975, n. 5;

Visti gli articoli 7 e 8 del decreto del Presidente della Repubblica 3 dicembre 1975, n. 805;

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;

Visto l'articolo 2 della legge 7 agosto 1990, n. 241;

Visto l'articolo 7-bis del decreto-legge 10 giugno 1994, n. 357, convertito, con modificazioni, dalla legge 8 agosto 1994, n. 489;

Udito il comitato di settore per i beni archivistici nella seduta del 1° luglio 1992;

Udito il parere del Consiglio di Stato, espresso nell'adunanza generale del 25 luglio 1996;

Sulla proposta del Ministro per i beni culturali e ambientali, di concerto con il Ministro di grazia e giustizia, con il Ministro delle finanze e con il Ministro del tesoro;

Adotta il seguente regolamento:

1. Limiti, modalità e procedimenti tecnici per la riproduzione sostitutiva.

1. Per i privati la facoltà prevista dall'articolo 25 della legge 4 gennaio 1968, n. 15, di riproduzione sostitutiva dei documenti di archivio, delle scritture contabili compresi i libri giornali e degli inventari, della corrispondenza e degli altri atti di cui per legge è prescritta la conservazione, è esercitata, fatti salvi i limiti di cui all'articolo 2 del decreto del Presidente del Consiglio dei Ministri 11 settembre 1974, con le modalità ed i procedimenti tecnici stabiliti dal presente decreto.

2. Il procedimento di microfilmatura è disciplinato dal presente decreto.

3. I documenti d'archivio, sottoposti a riproduzione sostitutiva sono riprodotti su qualsiasi supporto tecnico previsto dalla legge, che dà garanzia di fedeltà al documento riprodotto, di duplicabilità, di leggibilità, di resistenza dell'immagine a tentativi di alterazione e di stabilità nel tempo, in condizioni normali di conservazione.

4. Fatto salvo quanto disposto dall'articolo 7-bis, comma 9, del decreto-legge 10 giugno 1994, n. 357, convertito, con modificazioni, dalla legge 8 agosto 1994, n. 489, i procedimenti tecnici e le modalità della riproduzione e della autenticazione su supporti diversi da quello previsto dal comma 2, sono stabiliti con decreto del Presidente del Consiglio dei Ministri, sentiti i Ministri per i beni culturali e ambientali, di grazia e giustizia, delle finanze e del tesoro, previo parere del comitato di settore per i beni archivistici.

2. Adempimenti preliminari all'esercizio della facoltà di riproduzione sostitutiva.

1. I privati che intendono avvalersi della facoltà di cui all'articolo 25 della legge 4 gennaio 1968, n. 15, inoltrano al soprintendente archivistico, competente per territorio, il relativo progetto di riproduzione sostitutiva.

2. Entro novanta giorni dalla presentazione, il soprintendente, esaminata la rispondenza del progetto stesso alla normativa in vigore lo approva oppure lo respinge con provvedimento motivato.

3. Ove i documenti oggetto della riproduzione sostitutiva sono conservati in sedi dislocate in un ambito territoriale più ampio di quello regionale, i titolari dell'archivio inoltrano il progetto di riproduzione sostitutiva direttamente al Ministero per i beni culturali e ambientali - Ufficio centrale per i beni archivistici.

4. La relativa approvazione o il suo motivato rigetto è disposta dall'ufficio di cui al comma 3, previo parere del comitato di settore per i beni archivistici, entro centoventi giorni dalla data di presentazione del progetto stesso.

3. Distruzione dei documenti riprodotti.

1. Alla distruzione dei documenti di cui è stata eseguita la riproduzione sostitutiva si procede dopo avere effettuate le operazioni di autenticazione ai sensi dell'articolo 8, salvo per quei documenti per i quali l'amministrazione archivistica, in sede di approvazione del progetto, vieti la distruzione disponendone il ritiro e la conservazione a proprie spese.

2. I registri o i libri comunque denominati, non esclusi dall'applicazione dell'articolo 25 della legge 4 gennaio 1968, n. 15, ai sensi dell'articolo 2 del decreto del Presidente del Consiglio dei Ministri 11 settembre 1974, non possono essere riprodotti e distrutti se non sono esauriti.

4. Cartellinatura degli atti e dei documenti da riprodurre.

1. Gli atti e documenti destinati alla riproduzione sostitutiva sono oggetto di cartellinatura.

2. La cartellinatura consiste nella preparazione degli atti e documenti da riprodurre e nell'approntamento di idonei strumenti di consultazione, eventualmente integrati da codificazioni per l'elaborazione elettronica, che in base alle indicazioni apposte sui singoli atti e documenti ed a quelle inserite sul corrispondente supporto tecnico utilizzato per la riproduzione, consentono di rilevare la stretta connessione degli atti e documenti riprodotti con il loro raggruppamento (unità, serie o altro livello di aggregazione) e di reperire prontamente gli atti o i documenti da consultare o duplicare.

3. In particolare, dopo la individuazione della categoria dei documenti da riprodurre, si osservano le seguenti modalità:

a) le unità archivistiche sono numerate progressivamente nell'interno di ciascuna serie (o di altro livello di aggregazione), la cui indicazione va riportata sul frontespizio delle unità stesse;

b) gli atti e i documenti compresi in ciascuna unità archivistica sono ordinati e numerati, ed eventualmente codificati, secondo l'ordine cronologico ad iniziare dal documento meno recente, salvo che per quegli atti e documenti che per esigenze organizzative sono ordinati diversamente o sono legati in volume o riportati nel registro già numerati progressivamente, per i quali resta fermo il relativo ordine;

c) le pagine di cui si compone ciascun documento compreso nell'unità archivistica, o la medesima unità archivistica se questa è composta di un unico documento, sono numerate progressivamente;

d) l'indicazione della serie di appartenenza di ciascun atto o documento viene individuata da qualsiasi sistema di individuazione purché rispondente ai criteri dettati dal comma 2.

Per l'indicazione degli altri livelli di aggregazione archivistica eventualmente previsti sono adottati criteri analoghi;

e) la numerazione può essere effettuata manualmente o meccanicamente. Eventuali errori sono corretti annullando l'indicazione errata e ripetendo a fianco quella esatta;

f) ciascuna unità archivistica è descritta in un registro di serie, nel quale sono riportate le indicazioni atte ad identificarla (cioè denominazione del soggetto o ente tenuto a conservare l'archivio, denominazione della categoria dei documenti, denominazione ed estremi cronologici della serie o di altro livello di aggregazione, numero dell'unità archivistica, quantità dei documenti o delle pagine che la compongono) e quelle atte ad identificare le corrispondenti unità di riproduzione (numero di bobina o di altro complesso fotografico, numero iniziale e finale dei fotogrammi riproducenti la singola unità archivistica). Le indicazioni relative alle unità di riproduzione vanno previste anche per gli eventuali rifacimenti di cui all'articolo 7.

4. I registri di serie, prima dell'uso sono numerati progressivamente per ogni pagina e vidimati ai sensi e con le modalità previste dall'articolo 2215 del codice civile; contengono altresì, per ogni blocco di unità di riproduzione autenticate, le dichiarazioni del pubblico ufficiale di cui al comma 5 dell'articolo 8, complete della qualifica e delle generalità dello stesso.

5. Le predette indicazioni sono, in presenza di particolari tipologie documentarie, integrate con tutti gli altri dati eventualmente utili all'individuazione delle singole unità archivistiche.

6. Per la documentazione da riprodurre che non è raggruppata o raggruppabile in serie, il registro di serie contiene l'indicazione dei criteri di elencazione delle unità archivistiche.

5. Procedimento di microfilmatura.

1. Il microfilm sostitutivo degli atti e documenti dei quali si intende procedere alla distruzione è costituito da una pellicola negativa soggetta alle prescrizioni del decreto del Ministro per i beni culturali e ambientali 29 marzo 1979 pubblicato nella Gazzetta Ufficiale n. 206 del 28 luglio 1979, con il quale sono state approvate le caratteristiche della pellicola destinata alla fotoriproduzione sostitutiva dei documenti d'archivio.

2. Quale unità di riproduzione è assunta oltreché la bobina del tipo comunemente in commercio, qualsiasi altra pellicola negativa, di formato ridotto, purché atta a costituire un complesso collegabile mediante numerazioni o altri simboli che garantiscono l'univoca individuazione delle singole unità di riproduzione.

3. Le unità di riproduzione non sono impressionate sulla loro parte terminale per uno spazio sufficiente ai fini dell'apposizione dell'attestazione di autentica di cui all'articolo 8.

4. Il processo fotografico è effettuato a regola d'arte.

5. Le pellicole impressionate sono custodite in modo da garantirne la leggibilità e la stabilità in condizioni normali di conservazione.

6. Indicazioni da apporre nel negativo sostitutivo.

1. La pellicola è impressionata con le indicazioni sottospecificate:

a) denominazione del soggetto o ente tenuto a conservare l'archivio;

b) denominazione della categoria dei documenti;

c) denominazione ed estremi cronologici della serie o di altro livello di aggregazione;

d) numero o codice dell'unità di riproduzione, data dell'impressione, denominazione del laboratorio cui è affidato il procedimento di impressione;

e) numero dell'unità archivistica e quantità dei documenti o delle pagine che la compongono;

f) quantità e numero di documenti o di pagine mancanti, nonché di fogli bianchi o danneggiati.

2. Gli estremi di cui alle lettere a), b), c) e d) di cui al comma 1 costituiscono lo schedone generale di serie. Tale schedone è riprodotto sia sul secondo che sul penultimo fotogramma di ciascuna unità di riproduzione mentre sul primo e sull'ultimo fotogramma sono riprodotti i simboli internazionali di «inizio» e «fine» pellicola;

3. Gli estremi di cui alle lettere e) ed f) di cui al comma 1 costituiscono lo schedone particolare dell'unità archivistica. Tale schedone può essere sostituito dal frontespizio di ciascuna unità archivistica ed è riprodotto all'inizio di detta unità.

4. Quando l'unità archivistica non è contenuta integralmente nella medesima unità di riproduzione, lo schedone di cui alle lettere e) ed f) è riprodotto, con idonee indicazioni di collegamento, a chiusura dell'unità di riproduzione e all'inizio della successiva.

5. I fotogrammi sono numerati progressivamente per unità di riproduzione secondo le indicazioni di cui all'articolo 4, comma 3, lettera d).

6. Ciascuna unità di riproduzione è descritta in apposito registro nel quale sono riportati gli estremi di classificazione di cui alla lettera d) di cui al comma 1 e quelli idonei ad identificare le unità archivistiche in essa riprodotte.

7. I registri delle unità di riproduzione di cui al comma 6 sono, prima dell'uso, numerati progressivamente per ogni pagina e vidimati ai sensi e con le modalità previste dall'articolo 2215 del codice civile.

7. Collaudo.

1. La pellicola sostitutiva dei documenti d'archivio è sottoposta a collaudo.

2. Qualora al collaudo risultano errori di cartellinatura o di ripresa si provvede alle necessarie integrazioni e correzioni, fotografando i documenti non riprodotti o riprodotti nei fotogrammi errati o danneggiati in una o più unità di riproduzione, che hanno una propria numerazione e fanno parte integrante della serie di riproduzione cui si riferiscono.

3. Le unità di riproduzione riservate ai rifacimenti sono soggette alle prescrizioni del presente decreto.

4. Ciascuna unità di riproduzione riservata ai rifacimenti, al secondo e penultimo fotogramma, riporta accanto al proprio numero o al codice di individuazione, l'indicazione «rifacimenti», nonché i numeri o i codici delle unità di riproduzione cui le correzioni si riferiscono.

5. I rifacimenti sono eseguiti per ordine progressivo delle unità di riproduzione in cui sono contenuti i fotogrammi da ripetere e per ciascuna unità di riproduzione seguendo l'ordine progressivo dei fotogrammi errati. Il numero del fotogramma da sostituire è dato al rifacimento corrispondente. Il fotogramma relativo a un documento non riprodotto ha lo stesso numero, contrassegnato dalla lettera dell'alfabeto, del fotogramma che riproduce il documento immediatamente precedente nell'ordine di cartellinatura.

6. All'inizio del gruppo di fotogrammi che ne sostituiscono altri annullati della medesima unità di riproduzione sono riportate le indicazioni che contraddistinguono detta unità con la legenda «inizio rifacimento»; prima dei fotogrammi di ciascuna unità archivistica, è riprodotto lo schedone particolare con l'indicazione «inizio rifacimento».

7. Durante il collaudo sono annullati in maniera evidente ed indelebile, senza compromettere la resistenza della pellicola, i fotogrammi errati e in presenza di duplicati quelli tecnicamente peggiori.

8. Procedimento e modalità di autenticazione della pellicola sostitutiva.

1. La pellicola riprodotte gli atti e i documenti da sostituire ai sensi e per gli effetti dell'articolo 25 della legge 4 gennaio 1968, n. 15, è autenticata da pubblici ufficiali forniti di potestà certificativa, o da soggetti ad essi equiparati.
2. Il Presidente del Consiglio dei Ministri, indica, con proprio decreto, i ministri cui demandare il potere di attribuire a propri funzionari la potestà ad effettuare le attività di cui al presente articolo.
3. Il pubblico ufficiale incaricato dell'autenticazione verifica la conformità alle prescrizioni del presente decreto del procedimento di cartellinatura e di formazione della pellicola sostitutiva, procedendo all'esame delle unità di riproduzione e dei registri di cui all'articolo 4, comma 3, lettera f) e all'articolo 6, comma 6.
4. Eseguite le operazioni descritte nel comma 3, il pubblico ufficiale appone il proprio punzone nella parte dell'unità di riproduzione non impressionata, ai sensi dell'articolo 5, comma 3.
5. Delle operazioni descritte nei commi 3 e 4, il pubblico ufficiale dà atto mediante dichiarazione su ciascuna pagina del registro di cui all'articolo 4, comma 3, lettera f).
6. Il pagamento dei diritti di autenticazione è effettuato mediante apposizione, su ciascuna delle predette pagine, di una marca da bollo che il pubblico ufficiale annulla, secondo le modalità previste dall'articolo 14 della legge 4 gennaio 1968, n. 15.

9. Efficacia della pellicola sostitutiva.

1. La pellicola autenticata con il procedimento e le modalità previste dall'articolo 8 sostituisce, ai sensi e per gli effetti dell'articolo 25 della legge 4 gennaio 1968, n. 15, gli originali dei documenti riprodotti.
2. Dalla pellicola sostitutiva, autenticata ai sensi dell'articolo 8, sono tratte copie integrali o parziali. Per la formazione di tali copie sono ammessi tutti i procedimenti tecnici.

Autorità per l'Informatica nella Pubblica Amministrazione

Deliberazione AIPA 9 novembre 1995

Definizione delle regole tecniche per il mandato informatico

(G.U. 22 novembre 1995, n. 273)

L'Autorità per l'Informatica nella Pubblica Amministrazione

Visto l'articolo 2, comma 2, del decreto del Presidente della Repubblica 20 aprile 1994, n. 367, che prevede che l'Autorità definisca "le regole tecniche... affinché le evidenze informatiche possano essere validamente impiegate a fini probatori, amministrativi e contabili";

Precisato che per evidenza informatica si intende un messaggio elettronico, composto da dati utente e da codici universali, che viene validamente impiegato a fini probatori, amministrativi e contabili;

Vista la proposta all'uopo predisposta dagli uffici;

Delibera di dettare, a norma dell'articolo 2, comma 2, del decreto del Presidente della Repubblica 20 aprile 1994, n.367, le regole tecniche per il mandato informatico di seguito riportate.

Regole tecniche per il mandato informatico

1. Protocollo di trasmissione.

I dati vengono trasmessi, di regola, attraverso linee di telecomunicazione: il protocollo di trasmissione adottato è quello riportato nella norma CCITT X.25 e successive evoluzioni.

2. Regole sintattiche.

Le regole sintattiche di trattamento delle evidenze informatiche devono conformarsi allo standard

UN/EDIFACT mantenuto da UN/ECE, emesso da ISO e ripubblicato da CEN per l'Europa, e pertanto la norma di riferimento è la EN 29735:1992 (ISO 9735) e successive evoluzioni, incluso ISO 9735 Amendment 1:1992 (estensione del repertorio caratteri).

3. Directory UN/EDIFACT.

I messaggi da utilizzare dovranno essere conformi alle specifiche definite nelle directory UNTDID e scelti tra:

i messaggi allo status 2 (messaggi standard) dell'ultima directory pubblicata, altrimenti tra i messaggi allo status 2 di directory precedenti all'ultima pubblicata ma non oltre la UNTDID Version S.93.A inclusa, altrimenti tra i messaggi allo status 1 dell'ultima directory o di directory precedenti all'ultima pubblicata, ma non oltre la UNTDID Version D.93.A inclusa.

Qualora si renda necessario definire nuovi messaggi si fa riferimento a quanto specificato nel documento "UN/EDIFACT Message Design Guidelines"; le strutture di dati dovranno conformarsi, ove possibile, a quelle definite nelle directory UN/EDIFACT di "segmenti dati" e "data element". Tali messaggi dovranno essere sottoposti all'Autorità per una verifica e per un'eventuale, successiva, istruttoria per la standardizzazione.

4. Sicurezza dell'Interscambio

4.1 Servizi

Per quanto attiene la sicurezza dell'interscambio dovranno essere realizzati i seguenti servizi:

Autenticazione dell'origine;

Non ripudio (invio e ricezione);

Integrità del contenuto;

Integrità della sequenza dei messaggi.

I suddetti servizi dovranno essere realizzati in conformità al DRAFT UN/ECE R.1026 Addendum 1-4 emesso dalle Nazioni Unite nell'aprile 1994, che rappresenta attualmente il documento di riferimento per la realizzazione della sicurezza in UN/EDIFACT.

Qualora le amministrazioni interessate ritengano necessario realizzare anche il servizio di "CONFIDENZIALITÀ DEL CONTENUTO" (RISERVATEZZA), per il quale non è disponibile alla data alcuno standard UN/EDIFACT di riferimento, la sua realizzazione dovrà avvenire secondo la seguente modalità:

Realizzazione del servizio per la RISERVATEZZA, contestualmente agli altri servizi di sicurezza, nell'ambito dello stesso messaggio.

I dati oggetto del servizio per la riservatezza sono contenuti in tutti i segmenti del messaggio

(Tecnica Header - Trailer). Gli elementi di sicurezza necessari alla decrittazione dei segmenti utente sono inseriti in appositi segmenti posti all'inizio del messaggio e prima della parte crittografata.

Per particolari condizioni, e previa autorizzazione dell'Autorità, è possibile adottare la seguente modalità alternativa:

Realizzazione del servizio per la RISERVATEZZA mediante interscambio EDIFACT.

Il messaggio contenente i dati applicativi viene inviato crittografato e l'interscambio avviene utilizzando uno dei meccanismi di comunicazione descritti al punto 5 (Meccanismo di comunicazione). Le informazioni per la decifrazione del messaggio interscambiato sono inviate, tramite messaggio AUTACK, assieme alle altre informazioni necessarie a realizzare i servizi di sicurezza indicati in precedenza.

4.2 Gestione delle chiavi

Per la gestione delle chiavi sarà necessario individuare i cinque distinti ruoli appresso riportati:

- Utente;
- Autorità di certificazione;
- Directory;
- Generatore della chiave;
- Autorità di registrazione.

Per quanto riguarda sia le modalità di gestione delle chiavi sia le competenze da attribuire ai singoli ruoli, saranno specificate appropriate regole tecniche da parte dell'Autorità.

Nel caso di interscambio tra un numero limitato di entità, e in attesa delle relative regole tecniche, è consentito l'uso di un meccanismo bilaterale concordato tra le parti. A tal fine, le modalità di gestione delle chiavi possono essere distinte per:

- Chiavi asimmetriche:

Generazione: avviene a cura di ciascuna entità;

Distribuzione: ciascuna entità invia la chiave pubblica soddisfacendo i requisiti di autenticità, integrità e non ripudio dell'origine e della destinazione.

Chiavi simmetriche:

Generazione: avviene a cura di una delle entità, o dalle entità in concorso, rispettando le procedure con-cordate

e sottoscritte;

Distribuzione: avviene come per le chiavi asimmetriche realizzando, in aggiunta, il soddisfacimento del requisito della confidenzialità.

Le chiavi dovranno essere rinnovate periodicamente e con un intervallo di tempo concordato tra le amministrazioni interessate rispettando i requisiti sopra esposti.

5. Meccanismo di comunicazione

Il meccanismo di comunicazione che dovrà essere utilizzato per lo scambio delle evidenze informatiche dovrà essere conforme alla norma CCITT X.400 versione 88 (ISO/IEC 10021-1-7:1988) e successive evoluzioni.

L'interchange EDIFACT dovrà essere trasferito con approccio P2.

Alternativamente potrà essere utilizzato il protocollo riportato nella norma CCITT X.435 (ISO/IEC 10021-8,9) conosciuto anche con la denominazione Pedi.

6. Modelli di accordo (contratto EDI)

Per gli accordi bilaterali si dovrà fare riferimento alla raccomandazione della commissione della Comunità Europea del 19 ottobre 1994, che specifica lo schema contrattuale per la regolamentazione degli aspetti tecnici e legali dell'interscambio tra le parti.

Quando saranno disponibili altre norme che soddisfino le esigenze relative al mandato informatico l'Autorità provvederà ad emanare le relative regole tecniche.

Il Presidente:
Rey

Autorità per l'Informatica nella Pubblica Amministrazione

Deliberazione 30 luglio 1998

Regole tecniche per l'uso di supporti ottici

(Art. 2, comma 15, della legge 24 dicembre 1993, n. 537)

(G.U. 19 agosto 1998, n. 192)

L'Autorità per l'Informatica

Visto l'art. 2, comma 15, della legge 24 dicembre 1993, n. 537, che prevede che gli obblighi di conservazione e di esibizione di documenti, per finalità amministrative e probatorie, previsti dalla legislazione vigente, si intendono soddisfatti anche se realizzati mediante supporto ottico, purché le procedure realizzate siano conformi a regole tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione;

Vista la propria deliberazione n. 15 del 28 luglio 1994, pubblicata nella Gazzetta Ufficiale, n. 216 del 15 settembre 1994, con cui, in attuazione del predetto art. 2, comma 15, della legge 24 dicembre 1993, n.537, sono state dettate le regole tecniche per l'uso dei supporti ottici;

Visto il decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni nella legge 8 agosto 1994, n. 489, e in particolare l'art. 7 bis, comma 4, il quale prevede che le scritture contabili ed i documenti, cui si riferisce l'art. 2220 del codice civile, possono essere conservati sotto forma di registrazione su supporti di immagini, sempreché le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili;

Visto il comma 9 dello stesso art. 7 bis del richiamato decreto-legge n. 357 del 1994, il quale prevede che le citate disposizioni relative alle scritture obbligatorie di cui all'art. 2220 del codice civile si applicano anche a tutte le scritture e documenti rilevanti ai fini delle disposizioni tributarie e che, con decreto del Ministro delle finanze, sono determinate le modalità per la loro conservazione su supporti di immagine;

Visto l'art. 3, comma 147, lettera c) della legge 28 dicembre 1995, n. 549, che delega al Governo l'emanazione, ai sensi dell'art. 17, comma 2, della legge 23 agosto 1988, n. 400, di regolamenti al fine di semplificare le modalità di conservazione delle scritture contabili e degli altri documenti previsti dalle norme fiscali attraverso l'uso di supporti ottici e magnetici, in conformità ai criteri dettati dall'Autorità per l'informatica nella pubblica amministrazione, a condizione che sia possibile la lettura e la stampa contestualmente alla richiesta avanzata dagli uffici competenti ed in presenza di impiegati degli stessi uffici;

Visto l'art. 15, comma 2, della legge 15 marzo 1997, n. 59, per cui "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati su supporto informatico, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici o telematici, sono validi e rilevanti a tutti gli effetti di legge", rinviando a specifici regolamenti da emanarsi ai sensi dell'art. 17, comma 2, della legge 23 agosto 1988, n. 400, la definizione dei criteri e le modalità di applicazione;

Visto il decreto del Presidente della Repubblica 10 novembre 1997, n. 513, 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";

Ritenuto pertanto opportuno di sostituire integralmente la deliberazione n. 15 del 28 luglio 1994 con altra finalizzata a dettare sia le regole tecniche che criteri attuativi, che soddisfino le esigenze connesse all'evoluzione tecnologica e nel contempo realizzino modalità semplificate ed uniformi per l'archiviazione ottica dei documenti;

Delibera

La presente deliberazione sostituisce integralmente la precedente deliberazione n. 15 del 28 luglio 1994 contenente le regole tecniche per l'uso dei supporti ottici, la quale cessa di avere efficacia dal momento dell'emanazione delle seguenti disposizioni:

Art. 1 - Definizioni

1. Ai fini della presente Deliberazione si intende per:

- a) *Archivio*: l'insieme costituito da uno o più supporti di memorizzazione, univocamente identificati, contenenti un insieme di documenti registrati. Esso può inoltre contenere informazioni di qualsiasi tipo utili per la gestione dei documenti.
- b) *Supporto di memorizzazione*: il mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso.
- c) *Classe di supporti di memorizzazione*: l'insieme di supporti di memorizzazione aventi caratteristiche simili dal punto di vista meccanico, della capacità, delle prestazioni e del costo.
- d) *Documento registrato*: un documento, costituito da una o più pagine, identificato univocamente nell'ambito dell'archivio da un opportuno codice, assegnato al momento della sua prima archiviazione, che permetta la sua gestione in modo unitario senza alcuna dipendenza dal supporto di memorizzazione. Per ciascun documento registrato l'archivio contiene almeno una registrazione; nel caso di più registrazioni, queste possono essere contenute all'interno di uno o più supporti di memorizzazione.
- e) *Rappresentazione digitale* di un documento è una sequenza di simboli binari a partire dalla quale è possibile, attraverso opportuni strumenti hardware e software, la presentazione del documento stesso nella sua interezza.
- f) *Istanza* di un documento registrato è il risultato di una operazione di archiviazione effettuata a fronte del corrispondente documento d'origine. Ciascuna istanza di un documento registrato è individuata, nell'ambito di questo, dal numero d'ordine con cui è stata generata.
- g) *Versione* di una istanza di documento registrato è l'insieme costituito dalla rappresentazione digitale del documento e da una serie di informazioni di controllo necessarie per garantire la sua integrità e reperibilità. Si hanno versioni differenti quando le rappresentazioni digitali del documento in esse contenute non coincidono. La versione iniziale è generata dall'archiviazione, quelle successive sono prodotte da operazioni di riversamento in cui viene modificata la rappresentazione digitale del documento. Ciascuna versione è individuata, nell'ambito della medesima istanza, dal numero d'ordine con cui è stata generata.
- h) *Registrazione*: l'insieme di dati binari scritti durante un'operazione di archiviazione o di riversamento. Ciascuna registrazione presente in un supporto di memorizzazione è univocamente individuata dal numero d'ordine con cui essa è stata effettuata. Una registrazione contiene la rappresentazione digitale del documento, che corrisponde ad una versione di una istanza di un documento registrato. Ad essa è associata una marca di controllo attraverso cui viene garantita la sua integrità ed autenticità. Nel caso in cui si utilizzino tecniche di cifratura per proteggere documenti riservati, la marca di controllo è calcolata sopra la rappresentazione digitale in chiaro, ossia non cifrata, del documento.

- i) *Archiviazione*: l'operazione che genera, su di un supporto di memorizzazione, una registrazione contenente la versione iniziale di una istanza di un documento registrato. Per il medesimo documento l'operazione può essere ripetuta più volte allo scopo di correggere eventuali errori avvenuti durante il processo di archiviazione. La prima archiviazione di un documento genera il corrispondente documento registrato e quindi l'istanza iniziale di questo; ogni successiva reiterazione dell'operazione genera una sua nuova istanza del medesimo documento registrato che annulla la precedente. Pertanto, per ciascun documento, l'archivio contiene un'istanza attiva, quella generata dall'ultima archiviazione, ed eventualmente una o più istanze cancellate.
- j) *Riversamento* di un documento registrato è un'operazione che, a partire da una registrazione, ne genera una nuova sul medesimo oppure su di un altro supporto di memorizzazione, contenuto nello stesso archivio. L'operazione può avvenire con o senza modifica della rappresentazione digitale del documento archiviato. Nel secondo caso il riversamento opera una semplice duplicazione, nel primo viceversa produce una nuova versione per l'istanza del documento contenuta nella registrazione sorgente.
- k) *Presentazione* di un documento registrato è l'operazione che consente di visualizzare il documento originale, nonché di ottenerne copia anche su supporto cartaceo.
- l) *Presentabilità di una versione*: una versione è presentabile se è possibile effettuare la presentazione del documento registrato a partire dalla rappresentazione digitale del documento in essa contenuta.
- m) *Accessibilità di una versione*: una versione è accessibile se è possibile recuperare dal supporto di memorizzazione la rappresentazione digitale del documento e verificarne la congruenza con la marca di controllo ad essa associata.
- n) *Presentabilità di una istanza*: un'istanza è presentabile solo se nell'archivio esiste almeno una sua versione presentabile.
- o) *Accessibilità di una istanza*: un'istanza è accessibile solo se tutte le sue versioni presenti nell'archivio sono accessibili.
- p) *Tipo* di una registrazione è una informazione che ne specifica il ruolo nell'archivio. I valori possibili sono:
- 1) Archiviazione normale: la registrazione contiene la versione iniziale della prima istanza di un documento registrato.
 - 2) Archiviazione sostitutiva: la registrazione ne sostituisce un'altra risultata non corretta; essa perciò contiene la versione iniziale di una nuova istanza del documento registrato, che sostituisce l'istanza precedente
 - 3) Archiviazione cancellata: la registrazione contiene una rappresentazione digitale del documento che è risultata imperfetta ed ha perciò dato origine ad un'archiviazione sostitutiva. Essa contiene la versione iniziale di un'istanza del documento archiviato.
 - 4) Riversamento diretto: la registrazione ne duplica un'altra presente nell'archivio e, pertanto, contiene la medesima versione della medesima istanza presente nella registrazione sorgente.
 - 5) Riversamento sostitutivo: la registrazione deriva da un riversamento con modifica della rappresentazione digitale del documento, quindi contiene la versione successiva dell'istanza presente nella registrazione sorgente.
- q) *Cifrario asimmetrico* è un sistema di cifratura che utilizza chiavi diverse per le operazioni di codifica e decodifica, delle quali una, detta chiave privata, è destinata a restare segreta, l'altra, denominata chiave pubblica, ad essere divulgata. Gli algoritmi utilizzati devono essere conformi all'appendice D della norma ISO 9594-8. È altresì possibile utilizzare gli algoritmi previsti dalla normativa riguardante la sottoscrizione digitale dei documenti informatici. Le chiavi utilizzate debbono avere una lunghezza minima di 1.024 bit. La validità della chiave non può superare i due, tre e cinque anni, se

la lunghezza è pari rispettivamente a 1.024, 1.536 e 2.048 bit. Nel caso di chiavi certificate da un certificatore riconosciuto, la validità corrisponde a quella specificata dal certificato da esso rilasciato.

r) *Firma digitale* è il risultato della procedura informatica che consente di verificare la riferibilità soggettiva e l'integrità di una sequenza di simboli binari. Si ottiene mediante l'operazione di cifratura effettuata, conformemente alla norma ISO/IEC DIS 9796-2, con un cifrario asimmetrico, sopra l'impronta della sequenza di simboli binari utilizzando la chiave privata del soggetto. È consentito l'uso di firme digitali conformi alla normativa riguardante la sottoscrizione digitale dei documenti informatici.

s) *Impronta* di una sequenza di simboli binari è un'ulteriore sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di una funzione di hash tra quelle definite nella norma ISO/IEC DIS 10118-3 o comunque previste dalla normativa riguardante la sottoscrizione digitale dei documenti informatici, purché generanti impronte di dimensione conforme a quanto richiesto nella successiva lettera x) per le marche di controllo.

t) *Certificato* è il risultato della procedura informatica atta a garantire in modo verificabile l'attribuzione di una chiave di un cifrario ad un soggetto. Esso deve essere conforme alla norma ISO/IEC 9594-8 e successive estensioni. È possibile utilizzare qualsiasi certificato previsto dalla normativa riguardante la sottoscrizione digitale dei documenti informatici.

u) *Marca temporale* di una sequenza di simboli binari è essa stessa una sequenza di simboli binari, generata da un apposito servizio, che attribuisce data certa all'esistenza della prima sequenza garantendone nel contempo l'integrità.

v) *Marca di controllo* di una sequenza di simboli binari è un dato di controllo contenente le informazioni necessarie per verificarne l'integrità ed autenticità. Essa comprende:

1) l'indicazione della funzione di hash utilizzata per il calcolo dell'impronta primaria della sequenza di simboli binari cui la marca di controllo si riferisce.

2) il codice della funzione di hash indicata al punto precedente secondo la codifica specificata nella norma ISO/IEC DIS 9796-2.

3) l'impronta primaria della sequenza di simboli binari cui la marca di controllo si riferisce, calcolata con una delle funzioni previste nella precedente lettera u) che generi valori ad almeno 160 bit.

4) l'indicazione della funzione di hash utilizzata per il calcolo dell'impronta secondaria della sequenza di simboli binari cui la marca di controllo si riferisce.

5) il codice della funzione di hash indicata al punto precedente secondo la codifica specificata nella norma ISO/IEC DIS 9796-2.

6) l'impronta secondaria della sequenza di simboli binari cui la marca di controllo si riferisce, calcolata con una delle funzioni previste nella precedente lettera u) che generi valori ad almeno 160 bit e sia diversa da quella utilizzata per il calcolo dell'impronta primaria.

w) *Pubblico ufficiale*, ad eccezione dei casi per i quali possono essere chiamate in causa le altre figure previste dal comma 2, art. 14 della legge 4 gennaio 1968, n. 15, deve intendersi il notaio.

x) *Certificatore* è il soggetto pubblico o privato che certifica la chiave pubblica di un cifrario asimmetrico, rilasciando il certificato che rende pubblico, e che pubblica ed aggiorna gli elenchi dei certificati sospesi e di quelli revocati.

Art. 2 - Tipi di supporto utilizzabili

Per l'archiviazione dei documenti possono essere utilizzati i supporti per i quali l'operazione di scrittura comporta una modifica permanente ed irreversibile delle caratteristiche del supporto stesso. Sono pertanto esclusi i supporti per i quali esista una

tecnica per annullare l'effetto dell'operazione di scrittura anche nel caso che tale tecnica richieda l'uso di dispositivi diversi da quelli installati nel sistema di archiviazione.

2. Gli obblighi di conservazione di documenti previsti dalla legislazione vigente si ritengono soddisfatti e l'uso della relativa tecnologia è consentito senza preventiva autorizzazione, sempreché il tutto venga realizzato nel rispetto di quanto previsto dalla presente deliberazione.

Art. 3 - Standard applicabili

1. Il tipo di supporto e l'organizzazione dei dati utilizzati dal sistema di archiviazione debbono essere conformi alle norme nazionali o internazionali stabilite da organismi di normazione ufficialmente riconosciuti, che siano applicabili alla classe di supporti di memorizzazione utilizzati dal sistema e pubblicati al momento della sua acquisizione. Non sono considerate applicabili norme per le quali siano disponibili solo prodotti conformi provenienti da un unico fornitore. L'obbligo di conformità indotto dalla presenza di norme applicabili ad una classe di supporti di memorizzazione non riguarda classi di supporti diverse.

2. Il sistema deve comunque garantire la possibilità di riversamento dei documenti memorizzati nei principali formati previsti dalle norme nazionali o internazionali, comunque almeno su supporti conformi alla norma ISO 9660 ed almeno nei formati CGM e TIFF.

Art. 4 - Identificazione dei supporti

1. I supporti utilizzati per l'archiviazione debbono essere univocamente individuati. Ciò può avvenire sia attraverso codici univoci apposti in sede di fabbricazione, sia attraverso l'eventuale mappa dei difetti presenti sopra la superficie del supporto stesso, sia attraverso l'apposizione in modo indelebile sul supporto stesso, da parte del responsabile dell'archiviazione, di un codice identificativo autenticato da un pubblico ufficiale.

Art. 5 - Adempimenti del fornitore

1. Il fornitore è tenuto a certificare la conformità del sistema di archiviazione alle regole tecniche contenute nella presente deliberazione e, in particolare, alle norme nazionali o internazionali che siano applicabili secondo l'art. 3.

2. Il fornitore dei supporti di registrazione deve ugualmente certificare la conformità dello stesso supporto ai requisiti richiesti dall'art. 2.

3. Il fornitore del software di archiviazione è chiamato anch'esso a certificare la conformità di detto

software alle funzioni previste dalla presente deliberazione. In particolare, oltre alle funzionalità previste dall'art. 7, questo deve:

a) gestire le fasi che vanno dalla cattura dell'immagine alla sua memorizzazione senza consentire alcuna alterazione dell'immagine stessa;

b) visualizzare, stampare e riversare i documenti archiviati su supporto di memorizzazione senza consentire alterazioni del loro contenuto;

c) verificare la corrispondenza tra la rappresentazione digitale di un documento e la corrispondente

marca di controllo.

Art. 6 - Tipi di documento archiviabili

1. La conservazione su supporto ottico è prevista per le tipologie di documenti appresso indicati, secondo le modalità per ciascuna specificate:

a) documenti cartacei: tali documenti possono presentarsi sia come originali che come copie. Per gli

originali la formazione sul supporto di memorizzazione avviene, successivamente all'acquisizione in formato immagine, con il processo di autenticazione previsto all'art. 11.

Tale processo di autenticazione non è richiesto per i documenti in copia, la cui formazione su supporto di memorizzazione avviene con la sola acquisizione per immagine. Il processo di autenticazione non è richiesto anche per quei documenti originali al cui contenuto possa

risalirsi attraverso altre scritture o documenti di cui sia obbligatoria la tenuta, anche se in possesso da parte di terzi;

b) documenti formati all'origine su supporto informatico: i documenti formati direttamente su supporto informatico possono essere trasferiti sul supporto di memorizzazione, senza passaggio su supporto cartaceo, in un formato conforme allo standard SGML, oppure in uno dei seguenti formati: PDF, AFP e Metacode. È altresì possibile la conservazione di tali documenti come puro testo purché questo ne rappresenti integralmente ed in maniera non ambigua il contenuto. Deve essere in ogni caso definito univocamente il set di caratteri utilizzato, del quale deve essere contestualmente registrata l'immagine, e, qualora la formattazione non sia già implicitamente contenuta nel formato del documento, debbono essere specificate almeno la divisione in righe e pagine e la dimensione delle spaziature. Un documento formato secondo i precedenti requisiti costituisce la rappresentazione digitale del documento archiviato. È inoltre consentita l'archiviazione dei documenti formati all'origine su supporto informatico attraverso la conservazione della corrispondente immagine ottenuta per conversione diretta dal formato testuale; è possibile conservare sul medesimo supporto anche il testo del documento per scopi gestionali e documentali.

Art. 7 - Contenuti obbligatori del supporto di memorizzazione

1. Per ogni registrazione deve essere memorizzato, sul medesimo supporto, un file di controllo, indicato come "file di controllo della registrazione", che riporti almeno le seguenti informazioni:

- a) numero identificativo della registrazione;
- b) tipo di registrazione;
- c) codice identificativo del documento registrato;
- d) numero di istanza;
- e) numero di versione;
- f) codice identificativo del supporto contenente la registrazione sorgente o sostituita;
- g) numero identificativo della registrazione sorgente o sostituita;
- h) numero di istanza sorgente;
- i) numero di versione sorgente;
- l) nome e tipologia del file contenente la rappresentazione del documento;
- m) tipologia del documento;
- n) indici assegnati al documento registrato;
- o) nominativo del soggetto che effettua l'operazione;
- p) nominativo del responsabile dell'archiviazione;
- q) data ed ora di effettuazione dell'operazione;
- r) marca di controllo della rappresentazione digitale del documento;
- s) coppia di firme digitali del soggetto che effettua l'operazione, calcolate a partire dalle impronte primaria e secondaria contenute nella precedente marca di controllo;
- t) certificato della chiave pubblica necessaria per la verifica delle precedenti firme digitali.

La registrazione dei documenti deve essere effettuata in modo tale da preservare la loro individualità, onde consentire lo scorporo di un documento dagli altri.

2. All'atto della chiusura del supporto di memorizzazione deve essere generato su di esso un file, indicato come "file di chiusura", che deve risultare successivo all'ultima registrazione presente e contenere le seguenti informazioni:

- a) identificativo del supporto di memorizzazione d'origine;
- b) indicazione della casa produttrice del supporto d'origine;
- c) indicazione del fornitore del supporto d'origine;
- d) estremi della dichiarazione di conformità del supporto d'origine;
- e) identificativo del supporto di memorizzazione di sicurezza;
- f) indicazione della casa produttrice del supporto di sicurezza;
- g) indicazione del fornitore del supporto di sicurezza;

- h) estremi della dichiarazione di conformità del supporto di sicurezza;
 - i) data ed ora di effettuazione dell'operazione di chiusura;
 - l) numero di documenti registrati contenuti nel supporto;
 - m) numero di pagine formate;
 - n) numero delle registrazioni contenute;
 - o) nominativo del responsabile dell'archiviazione;
 - p) lista dei certificati, eventualmente generati dal responsabile dell'archiviazione, relativi alla chiave pubblica delle coppie usate per la certificazione delle altre chiavi utilizzate nel procedimento;
 - q) lista dei certificati, eventualmente generati dal responsabile dell'archiviazione, relativi alle chiavi da utilizzare per la verifica delle firme digitali contenute nel supporto di memorizzazione;
 - r) nominativo dell'operatore che effettua l'operazione di chiusura;
 - s) data dell'operazione di collaudo, di cui al successivo art. 9, e nominativo del soggetto che la esegue;
 - t) elenco delle registrazioni contenute nel supporto di memorizzazione, nel quale si riportano, per ciascuna di esse, le seguenti informazioni:
 - 1) numero identificativo della registrazione;
 - 2) tipo di registrazione;
 - 3) codice identificativo del documento registrato;
 - 4) numero di istanza;
 - 5) numero di versione;
 - 6) codice identificativo del supporto contenente la registrazione sorgente o sostituita;
 - 7) numero identificativo registrazione sorgente o sostituita;
 - 8) numero di istanza sorgente;
 - 9) numero di versione sorgente;
 - 10) marca di controllo contenuta nel relativo file di controllo;
 - 11) firme digitali contenute nel relativo file di controllo;
 - 12) firme digitali apposte per autentica secondo quanto previsto dall'art. 11 per i documenti per cui questa è richiesta.
 - u) elenco dei file di chiusura di supporti di memorizzazione eliminati eventualmente registrati nel supporto, riportando per ciascuno di essi:
 - 1) identificativo del supporto di memorizzazione;
 - 2) copia delle informazioni contenute nel file di controllo del file di chiusura;
 - 3) copia delle firme digitali apposte dal pubblico ufficiale durante la chiusura del supporto, secondo quanto previsto dal comma 4 dell'art. 10, a meno che non sia stata utilizzata l'autentica sostitutiva ivi indicata;
 - 4) copia del certificato necessario per la verifica delle firme digitali di cui al punto precedente.
3. Contestualmente alla registrazione del file di chiusura deve essere generato sul medesimo supporto il relativo file di controllo contenente le seguenti informazioni:
- a) marca di controllo del file di chiusura;
 - b) marca temporale generata a partire dall'impronta primaria contenuta nella precedente marca di controllo;
 - c) certificato della chiave pubblica necessaria per la verifica della precedente marca temporale;
 - d) coppia di firme digitali generate dal responsabile dell'archiviazione a partire dalle impronte primaria e secondaria contenute nella precedente marca di controllo;
 - e) certificato della chiave pubblica necessaria per la verifica delle precedenti firme digitali.

4. L'intero contenuto del supporto deve essere direttamente accessibile attraverso opportuni comandi di sistema che consentano almeno di:

a) visualizzare tutte le directory e sottodirectory presenti sul supporto di memorizzazione;
b) visualizzare tutti i file memorizzati sul supporto di memorizzazione, quindi le informazioni sopra

specificate, relative ai file di controllo delle registrazioni e di chiusura;

c) se applicabile alla tipologia di supporto, leggere in qualsiasi momento qualunque area del supporto di memorizzazione, anche quelle eventualmente dichiarate cancellate, e conoscere in ogni momento il numero delle tracce occupate e di quelle libere, sia relativamente alle tracce normali che a quelle di riserva.

Art. 8 - Responsabile dell'archiviazione

1. Il responsabile del procedimento di archiviazione:

a) definisce le caratteristiche ed i requisiti minimi del sistema di archiviazione in funzione della tipologia di documenti da trattare;

b) conserva, con l'impiego di procedure informatiche eseguite sui dati contenuti nell'archivio ottico,

relativamente ad ogni supporto di memorizzazione utilizzato, le informazioni appresso specificate:

1) la casa produttrice del supporto di memorizzazione;

2) l'identificativo del supporto di memorizzazione;

3) gli estremi di riferimento della dichiarazione di conformità;

4) la descrizione del contenuto del supporto di memorizzazione;

5) gli estremi identificativi della copia di sicurezza;

6) gli estremi identificativi del responsabile dell'archiviazione;

7) i nominativi degli operatori designati dal responsabile dell'archiviazione, con l'indicazione dei

compiti agli stessi assegnati;

c) mantiene, con le stesse modalità previste per i documenti formati all'origine su supporto informatico dall'art. 6, lettera b) un archivio del software utilizzato, in ogni sua versione. Per l'archiviazione dell'eseguibile dei programmi non si applicano le limitazioni di formato ivi previste;

d) garantisce la presentabilità ed accessibilità di tutte le istanze di ogni documento registrato contenuto nell'archivio, nonché la leggibilità del contenuto di ogni supporto di memorizzazione. In particolare, il responsabile è tenuto a:

1) adottare le misure necessarie per evitare la perdita o distruzione delle informazioni;

2) verificare periodicamente l'effettiva leggibilità del contenuto dell'archivio, provvedendo al riversamento del contenuto dei supporti non più idonei;

3) effettuare il riversamento del contenuto dei supporti tecnologicamente obsoleti;

e) verifica che il fornitore del sistema abbia certificato la rispondenza del sistema stesso alle specifiche tecniche contenute nella presente deliberazione, ed abbia fornito, attestandone la corretta funzionalità, i relativi programmi di gestione;

f) adotta le necessarie misure per la sicurezza fisica e logica del sistema di archiviazione;

g) cura, nell'ambito dell'attività di archiviazione, le operazioni di chiusura dei supporti, di copia e riversamento del loro contenuto e di esibizione di quanto formato su supporto di memorizzazione;

h) può delegare, per lo svolgimento delle attività di registrazione, riversamento e chiusura dei supporti di memorizzazione, soggetti che per competenza o esperienza garantiscano la corretta esecuzione delle operazioni, certificandone anche le chiavi di cifratura se queste non sono certificate da un certificatore riconosciuto;

i) effettua il collaudo previsto al successivo art. 9;

l) richiede la presenza di un pubblico ufficiale nei casi in cui è previsto il suo intervento, assicurando allo stesso sia l'assistenza sia le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

m) conserva le attestazioni eventualmente rilasciate dal pubblico ufficiale per le attività dallo stesso

svolte in ottemperanza a quanto previsto dalla presente deliberazione.

2. Il procedimento di archiviazione può essere delegato, in tutto o in parte, a soggetti che per specifica competenza ed esperienza assicurino la piena osservanza delle disposizioni contenute nella presente deliberazione e la corretta esecuzione delle istruzioni ricevute.

Art. 9 - Operazioni di collaudo e gestione degli errori

1. Il responsabile dell'archiviazione, prima della chiusura del supporto di memorizzazione, è tenuto ad effettuare un'operazione di collaudo finalizzata a riscontrare la correttezza degli adempimenti eseguiti, quindi la conformità tra quanto formato sul supporto e quanto oggetto di acquisizione.

2. Se nella fase di archiviazione di un documento si sono verificati errori, è possibile procedere ad una nuova registrazione dello stesso documento. La registrazione errata del documento viene conservata nell'archivio senza apportarvi alcuna modifica; essa costituisce una "istanza cancellata" del documento originariamente trattato. La nuova registrazione, che sostituisce l'istanza cancellata, viene a costituire "l'istanza attiva" del documento stesso. All'interno dell'archivio, costituito dall'insieme dei supporti ottici di memorizzazione elaborati, per ciascun documento archiviato esiste una ed una sola istanza attiva ed un numero di istanze cancellate. Tutte le istanze cancellate di un documento debbono essere conservate e mantenute accessibili nell'archivio. La sostituzione logica della registrazione errata si realizza attraverso l'inserimento di un riferimento ad essa nel file di controllo della registrazione generata dalla successiva nuova acquisizione. La validità di una registrazione è determinata dal valore assunto dal campo tipo nell'elenco delle registrazioni contenuto nel file di chiusura del supporto. Le istanze di ciascun documento, tutte contenute nell'archivio, possono trovarsi fisicamente su supporti diversi.

Art. 10 - Chiusura del supporto di memorizzazione

1. La chiusura del supporto di memorizzazione avviene successivamente all'operazione di collaudo previsto all'art. 9 e di autenticazione di cui all'art. 11. Di detta operazione il responsabile dell'archiviazione dà attestazione registrando sul supporto di memorizzazione il file di chiusura ed il relativo file di controllo previsti dall'art. 7.

2. Contestualmente alla chiusura di cui al precedente comma, il contenuto del supporto deve essere duplicato su un altro supporto di memorizzazione, che ne costituisce la copia di sicurezza, da conservarsi in luogo diverso. L'identificativo di tale supporto deve essere registrato nell'apposito campo del file di chiusura.

3. Nel caso di supporti di capacità elevata, l'operazione di chiusura può essere effettuata prima dell'effettivo riempimento del supporto. Qualora lo spazio disponibile residuo ecceda i 2 gigabyte è possibile considerare come parziale l'operazione di chiusura effettuata e procedere all'ulteriore riempimento del supporto con nuovi documenti. Solo per i documenti aggiunti dovrà essere effettuata un'ulteriore operazione di chiusura, nella quale sarà generato un nuovo file di chiusura con le medesime modalità previste dal comma 1. Contestualmente a ciascuna operazione di chiusura effettuata successivamente alla prima si dovrà procedere all'aggiornamento della copia di sicurezza duplicando su di essa i documenti aggiunti ed il relativo file di chiusura.

4. L'avvenuta operazione di chiusura, anche parziale, di un supporto di memorizzazione e la produzione della relativa copia di sicurezza sono certificate da un pubblico ufficiale mediante apposizione al file di chiusura delle proprie firme digitali, generate a partire dalle impronte primaria e secondaria, delle quali egli conserva copia. Tali firme, insieme con il

corrispondente certificato rilasciato da un certificatore riconosciuto, debbono essere registrate sul supporto di memorizzazione cui si riferiscono successivamente al file di controllo generato dal responsabile dell'archiviazione. La sottoscrizione digitale del file di chiusura da parte di un pubblico ufficiale può essere sostituita dall'autenticazione della firma apposta dal responsabile dell'archiviazione alla stampa contenente gli estremi di identificazione del supporto di memorizzazione ed il valore, rappresentato mediante un numerale esadecimale, delle due impronte presenti nella marca di controllo contenuta nel file di controllo del file di chiusura. Se da tale autenticazione è possibile determinare la data e l'ora in cui essa è stata effettuata, questa può sostituire anche la marca temporale prevista nel file di controllo del file di chiusura.

5. Nell'ambito delle amministrazioni pubbliche il ruolo del pubblico ufficiale è svolto dal Dirigente dell'ufficio responsabile alla tenuta, conservazione ed esibizione degli atti o documenti, od altri dallo stesso formalmente designati, sempreché non coincida con il responsabile dell'archiviazione.

Art. 11 - L'autenticazione dei documenti formati su supporti ottici:

1. I soli documenti cartacei per i quali è prevista all'art. 6 l'autenticazione devono essere singolarmente autenticati da un pubblico ufficiale, chiamato a verificare che quanto riprodotto, e quindi formato, sul supporto di memorizzazione, sia conforme al documento originale cartaceo oggetto di riproduzione. Tale formalità si intende assolta attraverso l'apposizione alla rappresentazione digitale di ciascun documento delle firme digitali del pubblico ufficiale generate a partire dalle impronte primaria e secondaria contenute nella marca di controllo presente nel relativo file di controllo. In alternativa è possibile certificare una lista dei documenti originali contenente il codice identificativo del supporto e, per ciascuno di essi, le seguenti informazioni:

a) numero identificativo della registrazione;

b) tipo di registrazione;

c) codice identificativo del documento registrato;

d) numero di istanza;

e) numero di versione;

f) rappresentazione esadecimale delle due impronte della rappresentazione digitale del documento

contenute nella marca di controllo presente nel file di controllo corrispondente.

2. Per tutti gli altri documenti, così come individuati all'art. 6, la loro conformità all'atto d'origine, sia cartaceo che informatico, viene attestata dal responsabile dell'archiviazione successivamente all'operazione di collaudo, contestualmente alla chiusura del supporto di memorizzazione, mediante la sottoscrizione digitale del file di chiusura attraverso le firme digitali presenti nel file di controllo di quest'ultimo.

3. Nell'ambito delle amministrazioni pubbliche l'operazione di autenticazione è effettuata dal Dirigente dell'ufficio responsabile alla tenuta, conservazione ed esibizione degli atti o documenti, od altri dallo stesso formalmente designati, sempreché non coincida con il responsabile dell'archiviazione.

Art. 12 - Riversamento dei documenti

1. Da una registrazione contenente una versione di un'istanza di un documento registrato, l'operazione di riversamento genera, sul medesimo o su un altro supporto di memorizzazione, una nuova registrazione contenente la medesima o una nuova versione della stessa istanza.

2. Solo nel caso di documenti per i quali è richiesta l'autenticazione di cui all'art. 11, se il riversamento genera una nuova versione, anche la versione sorgente deve essere conservata e mantenuta almeno accessibile nell'archivio.

3. Ogniqualevolta un'istanza di un documento viene sottoposta a riversamento, il responsabile dell'archiviazione deve verificare che rimanga assicurata la presentabilità di

tutte le altre istanze eventualmente presenti nell'archivio e procedere, se necessario, al loro riversamento.

Art. 13 - Riproducibilità dei documenti

1. Per tutto il tempo per il quale un supporto viene utilizzato, il responsabile dell'archiviazione deve assicurare la riproducibilità dei documenti archiviati in esso contenuti, ossia l'immediata riproduzione della loro immagine tanto sull'unità di visualizzazione che su quella di stampa del sistema di archiviazione.

2. La riproducibilità deve essere garantita tanto per la versione corrente dell'istanza attiva del documento archiviato che per quella di tutte le sue istanze cancellate. Deve inoltre essere garantita l'accessibilità di tutte le altre versioni di ciascuna istanza del documento archiviato di cui è obbligatoria la conservazione nell'archivio ai sensi del precedente art. 12.

Art. 14 - La distruzione dei supporti.

1. La distruzione del materiale cartaceo di cui sia stata effettuata l'archiviazione non può avvenire prima che il relativo supporto di memorizzazione sia stato chiuso secondo le modalità previste all'art. 10. Di tale distruzione è necessario informare, con comunicazione scritta fatta pervenire almeno sei mesi prima, il Soprintendente archivistico competente del Ministero per i beni culturali ed ambientali.

2. Un supporto di memorizzazione il cui contenuto sia integralmente disponibile nell'archivio mediante altri supporti può essere eliminato purché sia mantenuto nell'archivio il suo file di chiusura con la corrispondente marca di controllo e le firme digitali del pubblico ufficiale di cui all'art. 10 e all'art. 11, queste ultime eventualmente sostituite dalla stampa sostitutiva ivi prevista.

Art. 15 - L'esibizione

1. Tutte le istanze di un documento archiviato sul supporto ottico devono essere rese leggibili in qualunque momento presso l'utente del sistema e rese disponibili su supporto cartaceo.

2. Deve essere consentita l'esibizione dei documenti contenuti nell'archivio mediante supporto di memorizzazione almeno su supporto conforme alle norme ISO 9660 utilizzando per la rappresentazione digitale dei documenti almeno i formati CGM o TIFF. Nel supporto utilizzato per l'esibizione dei documenti, oltre ai file contenenti le rappresentazioni digitali dei documenti presenti nell'archivio, debbono essere inclusi i file di chiusura, con i relativi file di controllo, dei supporti di memorizzazione che li contengono, onde consentire la verifica della loro autenticità ed integrità.

3. È altresì consentita l'esibizione per via telematica purché sia garantita l'autenticità e l'integrità dei documenti registrati trasmessi.

4. Qualora la copia di un documento contenuto nell'archivio debba essere esibita su supporto cartaceo fuori dell'ambiente in cui è installato il sistema, è necessaria l'autenticazione da parte di un pubblico ufficiale solo se trattasi di documenti per i quali l'art. 6 prevede il processo di autenticazione.

Art. 16 - Le procedure operative

1. Ad ogni utente del sistema di archiviazione ottica di documenti è consentita l'adozione di procedure personalizzate ad integrazione, sempreché nel rispetto, delle norme di base stabilite dalla presente deliberazione.

2. Dette procedure devono essere pubbliche ed esibibili per stabilirne l'ammissibilità legale oltre che per accertare il corretto impiego del sistema.

3. Le sole pubbliche amministrazioni devono comunicare le procedure che intendono adottare all'Autorità per l'informatica nella Pubblica Amministrazione che ne conserva copia.

Art. 17 - Sistemi di archiviazione preesistenti

1. Le regole tecniche dettate con la deliberazione 28 luglio 1994, n. 15, continuano ad applicarsi ai sistemi di archiviazione ottica già esistenti o in corso di acquisizione al momento dell'entrata in vigore della presente deliberazione.

Art. 18 - Migrazione degli archivi preesistenti

I documenti archiviati in osservanza delle regole tecniche di cui alla deliberazione 28 luglio 1994, n. 15, possono essere trasferiti in un archivio conforme alla presente deliberazione se vengono acquisiti con le modalità previste per i documenti formati all'origine su supporto informatico, di cui all'art. 6, comma 1, lettera b).

Roma, 30 luglio 1998
Il Presidente: Rey

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 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.(G.U. 15 aprile 1999, n.87)

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

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

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:

- a. 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:
- a. 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:
 - a. 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

Il responsabile della sicurezza deve definire un piano per la sicurezza nel quale debbono essere contenuti almeno i seguenti elementi:

- a. 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.
2. 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.
2. È possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1 purché tra loro compatibili.
3. Sono compatibili tra loro le funzioni specificate nei sottoindicati raggruppamenti:
 - a. generazione e custodia delle chiavi, generazione dei certificati, personalizzazione dei dispositivi di firma, crittografia, sicurezza dei dati;
 - b. registrazione degli utenti, gestione del registro dei certificati, crittografia, sicurezza dei dati.

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.

CIRCOLARE 26 luglio 1999, n. AIPA/CR/22

Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Modalità per presentare domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

(Gazz.Uff. 2 agosto 1999, Serie Generale, n. 179)

Premessa

Il decreto del Presidente della Repubblica 10 novembre 1997, n. 513 ("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"), all'articolo 8, comma 3, stabilisce che le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio delle attività, in apposito elenco pubblico, consultabile in via telematica, predisposto e tenuto aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione. Tali certificatori devono essere dotati dei requisiti elencati nello stesso art.8, comma 3, del D.P.R. n.513/1997, e, per quanto riguarda le specifiche, devono osservare le regole tecniche da emanarsi ai sensi dell'articolo 3 dello stesso decreto.

Dette regole tecniche, emanate con il D.P.C.M. 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale n. 87 del 15 aprile 1999, all'articolo 16, comma 1, prevedono che: "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".

Con la presente circolare, resa disponibile anche sul sito Internet dell'AIPA: www.aipa.it, vengono illustrate le modalità con le quali le società interessate ad esercitare l'attività di certificatore dovranno inoltrare domanda all'AIPA.

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

La domanda, sottoscritta dal legale rappresentante della società, in plico chiuso con evidenza del mittente e con l'indicazione "Domanda per l'iscrizione nell'elenco dei certificatori", va indirizzata e fatta pervenire a:

Autorità per l'informatica nella pubblica amministrazione Via Solferino, 15 00185 ROMA

La consegna può avvenire tramite servizio pubblico o privato oppure a mano nelle ore d'ufficio (09.00-13.00 e 15.00-17.00) dei giorni dal lunedì al venerdì.

In quest'ultimo caso, verrà data formale ricevuta di consegna del plico.

Il testo della domanda e di tutti i documenti allegati originati dal richiedente, va predisposto 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 indicare:

- la denominazione della società;
- la sede legale;
- il o i rappresentanti legali;
- elenco dei documenti allegati.

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

Fatta salva la facoltà di avvalersi, nei casi consentiti, dell'autocertificazione di cui al D.P.R. 20 ottobre 1998, n. 403, alla domanda vanno allegati:

- a. copia autentica dell'atto costitutivo della società;
- b. statuto sociale vigente, certificato dalla competente CCIA (non anteriore a 90 giorni);
- c. certificato di iscrizione nel registro delle imprese (non anteriore a 90 giorni);
- d. dichiarazione del presidente del collegio sindacale, attestante l'entità del capitale sociale versato nonché l'ammontare e la composizione del patrimonio netto al momento della presentazione della domanda;
- e. situazione patrimoniale, predisposta e approvata dall'Organo amministrativo (non anteriore a 90 giorni) - (solo per le società già operative);
- f. relazione del collegio sindacale sulla situazione patrimoniale di cui alla lettera e;
- g. per le imprese registrate all'estero, documentazione equivalente a quella dei punti precedenti, a norma della legge n. 1253/1966*, legalizzata e tradotta in lingua italiana nelle forme e nei modi di cui alla legge n. 15/1968, salvo le eccezioni espressamente in essa previste;
- h. elenco nominativo dei componenti del consiglio d'amministrazione e del collegio sindacale, di eventuali amministratori delegati e del o dei direttori, dei soggetti con funzioni equivalenti a quelle del Direttore Generale, con l'indicazione dei relativi poteri. Ognuna delle suddette persone, dovrà risultare in possesso, all'atto della domanda, dei requisiti di onorabilità stabiliti dal decreto del Ministro del Tesoro, del Bilancio e della Programmazione economica 18 marzo 1998, n. 161, comprovato da:

- per i cittadini italiani residenti in Italia:

- dichiarazione, resa davanti a pubblico ufficiale, di possedere i requisiti di cui al decreto citato;
- certificato casellario giudiziale;
- certificato carichi pendenti presso la pretura e presso il tribunale;
- dichiarazione, resa davanti a pubblico ufficiale, di non esser stato destinatario, in altri Stati, di provvedimenti che importerebbero, secondo l'ordinamento italiano, la perdita dei requisiti di onorabilità di cui al decreto suddetto;

- per le persone che non rientrano nella categoria di cui al precedente alinea:

- dichiarazione, resa davanti a pubblico ufficiale, di possedere i requisiti di cui al decreto citato;
- certificati attestanti che la persona non è fallita o sottoposta a procedura equivalente, con parere legale che suffraghi l'idoneità dei certificati in questione; nel caso che il Paese di residenza non rilasci certificati, può essere accettata una dichiarazione sostitutiva resa davanti a pubblico ufficiale;
- le firme sulla documentazione vanno apposte a norma della legge n. 1253/1966.

Per entrambe le categorie, la prescritta certificazione antimafia sarà acquisita a cura dell'Autorità;

- i. copia della polizza assicurativa (o certificato provvisorio impegnativo) a copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali, a norma delle vigenti disposizioni;
- j. copia dell'ultimo bilancio con relativa certificazione, se la società è stata costituita da più di un anno. Se il bilancio non è stato certificato, la società dovrà allegare una dichiarazione di impegno a certificare il bilancio a partire dall'esercizio in corso al momento della presentazione della domanda;
- k. dichiarazione del presidente della società attestante la composizione dell'azionariato, per quanto nota, con indicazione, comunque, dei soggetti

partecipanti, in forma diretta o indiretta, al capitale sociale, in misura superiore al 5%;

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

Alla domanda vanno altresì allegati, secondo le modalità specificate nel seguito:

- m. copia del manuale operativo;
- n. copia del piano per la sicurezza;
- o. una relazione sulla struttura organizzativa;
- p. fermo restando quanto prescritto dall'articolo 18 del D.P.C.M. 8 febbraio 1999 sopra citato, dichiarazione di impegno a comunicare tempestivamente all'AIPA ogni variazione significativa delle soluzioni tecnico-organizzative adottate.

2. Requisiti tecnico-organizzativi da documentare

2.1 Manuale operativo

Il manuale operativo va strutturato in modo tale da essere integralmente consultabile per via telematica, come prescritto dall'articolo 45, comma 2, del D.P.C.M. sopra citato.

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 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 della società 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);
- k. procedura 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).

2.3 Organizzazione del personale

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

Va precisato, in particolare, a norma dell'articolo 16, comma 2, del D.P.C.M. 8 febbraio 1999, il profilo del personale responsabile della generazione 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, lett. c), del DPR n. 513/1997.

3. Requisiti tecnico-organizzativi da autocertificare

La società 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.

È 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'articolo 16, comma 3, del D.P.C.M. 8 febbraio 1999, di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato.

4. Modalità di esame delle domande

L'istruttoria delle domande e della relativa documentazione sarà svolta, sotto il controllo di un Membro dell'Autorità all'uopo designato, a cura degli uffici, con il supporto specialistico del Centro Tecnico di cui all'articolo 17, comma 19, della legge 15 maggio 1997, n. 127. Al termine dell'istruttoria, sulla richiesta di iscrizione nell'elenco dei certificatori sarà adottata

dall'Autorità, su proposta formulata dal Membro designato, motivata deliberazione di accoglimento o di reiezione ovvero, se ritenuta necessaria, di integrazione dell'istruttoria. La società, le cui domande di inserzione siano state oggetto di provvedimento di reiezione, non possono presentare una nuova istanza, se non siano trascorsi almeno 6 (sei) mesi dalla data di comunicazione del provvedimento stesso e, comunque, prima che siano cessate le cause che hanno determinato il non accoglimento della precedente domanda. Eventuali richieste di delucidazioni e/o chiarimenti potranno essere inoltrate al Direttore Generale dell'Autorità per l'informatica nella Pubblica Amministrazione.

Il Presidente: REY

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 ottobre 1999, n.437 Gazzetta Ufficiale n. 277 del 25-11-1999

Regolamento recante caratteristiche e modalita' per il rilascio della carta di identita' elettronica e del documento di identita' elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191. (GU n. 277 del 25-11-1999)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;

Visto l'articolo 2, comma 10, della legge 15 maggio 1997, n. 127,

come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n.191;

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

Visto il decreto del Presidente della Repubblica 10 novembre 1997, n. 513;

Vista la legge 31 dicembre 1996, n. 675;

Vista la legge 31 dicembre 1996, n. 676;

Visti gli articoli 3 e 4 del testo unico delle leggi di pubblica sicurezza approvato con regio decreto 18 giugno 1931, n. 773, e gli articoli 7, 288, 289, 290, 292, 293 e 294 del regio decreto 6 maggio 1940, n. 635;

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 attivita', 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;

Sentito il Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi, nell'adunanza del 10 maggio 1999;

Sulla proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica;

A d o t t a

il seguente regolamento:

Art. 1.

D e f i n i z i o n i

1. Ai fini del presente decreto si intende:

- a) per carta di identita' elettronica, il documento di riconoscimento personale rilasciato dal comune su supporto informatico;

- b) per documento d'identita' elettronico ai sensi dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come sostituito dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191, il documento analogo alla carta d'identita' elettronica e rilasciato dal comune prima del compimento del quindicesimo anno di eta';
- c) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- d) per dati identificativi della persona, il nome, il cognome, il sesso, la statura, la data e il luogo di nascita, gli estremi del relativo atto;
- e) per "altri dati" le informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attivita' amministrative e per l'erogazione di servizi al cittadino;
- f) per regole tecniche, le specifiche di carattere tecnico, organizzativo, funzionale e di sicurezza informatica, ivi compresa ogni disposizione che ad esse si applichi, relative alle tecnologie e ai materiali da utilizzare per la produzione e l'uso della carta di identita';
- g) per pubbliche amministrazioni, le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 3 febbraio 1993, n.29, e successive modificazioni.

Art. 2.

Rilascio della carta di identita' e del documento di identita' elettronico

1. La carta di identita' elettronica e il documento d'identita' elettronico sono rilasciati dal comune di residenza o d'iscrizione all'Anagrafe italiani residenti all'estero (AIRE) secondo le modalita' e le caratteristiche definite dal presente decreto e dal decreto di cui all'articolo 8.
2. Il documento d'identita' elettronico e' rilasciato a seguito della prima iscrizione anagrafica. Il suo rinnovo e' facoltativo. Se non rinnovato, il documento conserva validita' unicamente quale documento di attribuzione del codice fiscale.
3. Il Ministero delle finanze genera ed assegna alle persone fisiche il codice fiscale sulla base dei dati trasmessi dai comuni con le procedure di cui all'articolo 2, comma 2, del decreto del Presidente del Consiglio dei Ministri del 5 maggio 1994, pubblicato nella Gazzetta Ufficiale n. 148 del 27 giugno 1994. La procedura per la comunicazione ai comuni del codice fiscale e' disciplinata con decreto del Ministro dell'interno di concerto con il Ministro delle finanze, sentita l'Autorita' per l'informatica nella pubblica amministrazione.

Art. 3.

Forma, contenuto e funzione della carta d'identita' elettronica e del documento di identita' elettronico

1. La carta di identita' elettronica e il documento d'identita' elettronico devono contenere, con immediata visibilita' e memorizzati con modalita' informatiche di sicurezza sul documento ai sensi dell'articolo 8:
 - a) dati identificativi della persona;
 - b) codice fiscale;
 - c) dati di residenza;
 - d) cittadinanza;

- e) fotografia;
- f) eventuale indicazione di non validita' ai fini dell'espatrio;
- g) codice numerico identificativo del documento, codice del comune di rilascio, data del rilascio e data di scadenza;
- h) sottoscrizione del titolare o di uno degli esercenti la potesta' genitoriale o la tutela.

2. Il documento d'identita' elettronico puo' essere rilasciato anche senza la fotografia del titolare; in tal caso esso non e' valido per l'espatrio.

3. Il documento d'identita' elettronico (munito della fotografia del titolare) consente l'espatrio del minore di eta' inferiore ai dieci anni alle stesse condizioni previste dall'articolo 14, secondo comma, della legge 21 novembre 1967, n. 1185.

4. La carta d'identita' elettronica ed il documento d'identita' elettronico possono contenere i dati desunti dalle liste elettorali e comunque tutti quelli necessari per la certificazione elettorale e altri dati al fine di razionalizzare e semplificare l'azione amministrativa. Fra questi ultimi possono essere ricompresi anche dati amministrativi del Servizio sanitario nazionale nei limiti previsti da apposite linee guida emanate dal Ministero della sanita' di concerto con le altre amministrazioni interessate. Nel caso in cui i dati abbiano natura sensibile ai sensi dell'articolo 22 della legge 31 dicembre 1996, n. 675, questi possono essere inseriti nei documenti solo su richiesta dell'interessato, con le modalita' ivi previste.

5. I dati di cui al comma 1 sono trasmessi dal comune alla competente questura con le modalita' previste dal decreto di cui all'articolo 8.

Art.4.

Firma digitale e chiave biometria

1. La carta di identita' elettronica puo' contenere le informazioni e le applicazioni occorrenti per la firma digitale secondo quanto stabilito dalle regole tecniche di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, nonche' gli elementi necessari per generare la chiave biometrica.

Art. 5.

Validita' temporale della carta d'identita' e del documento d'identita' elettronico

1. La carta di identita' elettronica ha validita' di cinque anni. La medesima validita' ha il documento d'identita' elettronico privo della fotografia del titolare.

2. Il documento d'identita' elettronico munito della fotografia del titolare ha validita' di due anni.

Art.6.

Procedure di interdizione dell'operativita' elettronica in caso di smarrimento o furto della carta d'identita' elettronica e del documento d'identita' elettronico.

1. In caso di smarrimento o di furto sono previste procedure di interdizione dell'operativita' della carta d'identita' elettronica e del documento d'identita' elettronico, definite con il decreto del Ministro dell'interno di cui all'articolo 8.

Art.7.

Pagamenti informatici

1. La carta d'identita' elettronica puo' essere utilizzata anche per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni, previa definizione, d'intesa tra il comune interessato e l'intermediario incaricato di effettuare il pagamento, delle modalita' di inserimento e validazione dei dati necessari.

Art.8.

Regole tecniche e di sicurezza

1. Con il decreto del Ministro dell'interno di cui all'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, e successive modifiche, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione delle carte di identita' e dei documenti d'identita' elettronici di cui al presente decreto, specificate le caratteristiche fisiche e grafiche del supporto materiale, nonche' stabilite le modalita' di verifica da parte delle autorita' provinciali di pubblica sicurezza.
2. In particolare, le regole tecniche e di sicurezza devono riguardare le modalita' di compilazione, rilascio, aggiornamento e rinnovo dei documenti.
3. Le regole tecniche e di sicurezza sono adeguate in relazione alle esigenze dettate dalla evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno biennale a decorrere dalla data di entrata in vigore del presente decreto, salvaguardando l'utilizzabilita' dei documenti in corso di validita'.
4. Con il decreto di cui al comma 1 sono dettate le misure tecniche e di sicurezza finalizzate a garantire l'integrita', l'accessibilita' e la riservatezza delle informazioni contenute nel documento.

Art. 9.

Progetti di sperimentazione concernenti le modalita' di utilizzazione della carta di identita' elettronica e del documento elettronico per l'erogazione di ulteriori servizi o utilita'.

1. Le pubbliche amministrazioni possono sperimentare modalita' di utilizzazione della carta d'identita' elettronica e del documento d'identita' elettronico per l'erogazione di ulteriori servizi o utilita' attenendosi a quanto stabilito dal presente decreto e dal decreto di cui all'articolo 8.
2. Ai fini di cui al comma 1, le amministrazioni trasmettono al Ministero dell'interno il progetto di sperimentazione, contenente le specifiche tecniche, con l'indicazione della durata e del responsabile del progetto stesso.
3. Le amministrazioni proponenti possono avviare la sperimentazione decorsi trenta giorni dalla ricezione del progetto e in mancanza di determinazioni negative, da parte del Ministero dell'interno, in merito alla conformita' di progetto stesso al presente decreto e alle norme tecniche e di sicurezza di cui al decreto previsto dall'articolo 8. In caso di richiesta di chiarimenti il termine di trenta giorni e' sospeso e riprende a decorrere dalla ricezione degli elementi richiesti.

4. Fermo restando quanto previsto al comma 3, nel caso in cui la sperimentazione non risulti conforme alle finalita' del presente decreto e alle norme tecniche e di sicurezza di cui al decreto previsto dall'articolo 8, il Ministro dell'interno ne dispone la cessazione con provvedimento motivato. In tal caso, ai fini della ripresa della sperimentazione, l'amministrazione puo' presentare, secondo le modalita' di cui ai commi 2 e 3 del presente articolo, un nuovo progetto adeguandosi alle osservazioni formulate.

Art.10. Comitato di monitoraggio

1. Ferma restando la competenza del Ministro dell'interno per l'autorizzazione delle sperimentazioni, e' costituito un comitato di monitoraggio composto da diciotto membri, di cui tre della Presidenza del Consiglio dei Ministri, due del Dipartimento della funzione pubblica, quattro del Ministero dell'interno, due del Ministero delle finanze, due del Ministero della sanita', tre dei comuni, designati dalla conferenza Statocitta' e autonomie locali, due dell'Autorita' per l'informatica nella pubblica amministrazione.
2. Il comitato di cui al comma 1 svolge funzioni di collegamento tra la fase di sperimentazione e la fase di avvio a regime della carta d'identita' elettronica. In particolare il comitato svolge i seguenti compiti:
 - a) esprime pareri sulla validita' dei progetti avviati e dei servizi previsti nelle sperimentazioni;
 - b) effettua il monitoraggio dell'andamento delle sperimentazioni al fine di valutare e favorire le interrelazioni tra le stesse;
 - c) formula proposte per la migliore utilizzazione dei documenti elettronici, una volta conclusa la sperimentazione;
 - d) garantisce il raccordo delle sperimentazioni, nel caso in cui la carta d'identita' elettronica o il documento elettronico contengano dati amministrativi del Servizio sanitario nazionale, con la sperimentazione della tessera sanitaria nazionale.

Art.11.

Norme transitorie

1. Con decreto del Ministro dell'interno e' stabilita la data a decorrere dalla quale i comuni possono rilasciare la carta d'identita' elettronica in sostituzione dello stesso documento su supporto cartaceo, nonche' il documento d'identita' elettronico di cui al presente decreto.
2. Trascorsi cinque anni dalla data stabilita con il decreto di cui al comma 1, la carta d'identita' e' rilasciata soltanto su supporto informatico.
3. I comuni adottano un piano di sviluppo e revisione dei sistemi informativi automatizzati in attuazione di quanto stabilito dal presente decreto, attenendosi altresì alle disposizioni di cui agli articoli 20 e 21 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

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

Roma, 22 ottobre 1999

p. Il Presidente del Consiglio dei Ministri
Bassanini

Il Ministro dell'interno

Russo Jervolino

Il Ministro per la funzione pubblica

Piazza

Visto, il Guardasigilli: Diliberto

Registrato alla Corte dei conti il 22 novembre 1999

Registro n. 3 Presidenza del Consiglio dei Ministri, foglio n. 291

Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Premessa

Com'è noto, con il decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (recante: "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59") è stata introdotta nel nostro ordinamento la firma digitale. L'art. 8, comma 3, del citato D.P.R. n. 513/1997 stabilisce che le attività di certificazione sono effettuate da certificatori inclusi in apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto e aggiornato dall'Autorità per l'informatica nella pubblica amministrazione.

Con la circolare 26 luglio 1999, n. AIPA/CR/22 sono state stabilite le modalità con le quali le società interessate ad esercitare l'attività di certificatore devono inoltrare all'Autorità la domanda di iscrizione nell'elenco pubblico di cui al citato art. 8. In base a tale norma, i certificatori devono essere dotati di appositi requisiti e, per quanto riguarda le specifiche tecniche, essi devono osservare le regole di cui al D.P.C.M. 8 febbraio 1999.

La disciplina dei requisiti tecnici di sicurezza, pur riferendosi a standard internazionali, dà facoltà ad ogni certificatore di scegliere fra diverse tecnologie e strutture dei certificati. È pertanto possibile che, a causa di incompatibilità delle tecnologie e della struttura dei certificati utilizzati, soggetti che possiedono firme digitali certificate da differenti certificatori non siano in grado di scambiarsi tra loro documenti elettronici firmati. La problematica, peraltro, non ha trovato soluzione neppure con l'emanazione della direttiva europea sulla firma digitale, dove il problema dell'interoperabilità della firma digitale viene demandato ad un processo di standardizzazione internazionale a medio e lungo termine.

Ad un anno circa dalla pubblicazione delle regole tecniche, sette certificatori sono stati inclusi nell'elenco pubblico tenuto dall'Autorità e altri sono in procinto di iscriversi. Al fine perciò di garantire l'omogeneità operativa e la corretta interazione tra gli utenti che utilizzano la firma digitale, è stata avviata dall'Autorità un'azione di sensibilizzazione su queste tematiche nei confronti di tutti i certificatori iscritti, come pure nei confronti di quelli che hanno presentato domanda di iscrizione, affinché concordassero, in base all'art. 17 dell'allegato tecnico al D.P.C.M. 8 febbraio 1999, sulla necessità di individuare un documento di Linee guida che, ad integrazione degli standard esistenti, fornisse chiare indicazioni su come affrontare i problemi sulla struttura del certificato e sulle sue estensioni, sulla struttura delle liste di revoca e su quelle delle "buste elettroniche". Ciò al fine di colmare le lacune dovute ad un'interpretazione proprietaria di alcune regole sintattiche e semantiche degli standard, come peraltro già segnalato agli intermediari finanziari ed ai gestori dei sistemi di pagamento dalla Banca d'Italia, nell'ambito dell'analisi dei requisiti necessari al pieno e sicuro utilizzo della firma digitale nei trasferimenti elettronici di moneta.

La normativa vigente consente l'utilizzo di una serie di algoritmi e strutture dati, definiti in standard *de jure* o *de facto*. Non essendo possibile imporre regole precise, poiché ogni riferimento diretto ad una specifica tecnica potrebbe generare squilibri sul mercato o, addirittura, provocare a priori l'esclusione di alcuni fornitori, si ritiene comunque necessario fornire, con le presenti Linee guida, delle indicazioni di riferimento, anche tenendo conto dei suggerimenti provenienti dagli attori di mercato.

L'Autorità, per suo conto, ritiene che la soluzione del problema dell'interoperabilità della firma digitale è condizione necessaria per consentire il pieno utilizzo dei servizi di interoperabilità della Rete unitaria e per l'erogazione dei servizi diretti al cittadino.

Con la presente circolare, resa disponibile anche sul sito Internet dell'Autorità per l'informatica www.aipa.it, tenuto anche conto del disposto di cui all'art. 21 del D.P.C.M. 8 febbraio 1999 in tema di accordi tra certificatori, vengono appunto indicate le Linee guida per garantire l'omogeneità operativa e la corretta interazione tra gli utenti che utilizzano la firma digitale e la massima diffusione ed efficienza dei processi connessi alla firma digitale.

1. Il processo di firma digitale

Solo attraverso una piena interoperabilità tra i documenti elettronici firmati utilizzando certificatori diversi si garantisce piena efficienza e diffusione ai processi amministrativi utilizzando la firma digitale.

La soluzione al problema può essere duplice:

- a livello organizzativo, con un servizio fornito dai certificatori ed in grado di interpretare e tradurre i vari formati di firma;
- a livello tecnico, concordando uno standard per la P.A. italiana in termini di struttura del certificato e delle sue estensioni.

Appare evidente che la soluzione a livello tecnico è la più semplice in quanto non richiede sforzi realizzativi onerosi ed inoltre consente di seguire con sufficiente coerenza e tempestività le evoluzioni degli standard internazionali.

Ai fini di un primo livello base di interoperabilità sono da prendere in considerazione, oltre ai contenuti del certificato ed alla loro rappresentazione:

- le estensioni del certificato ed i loro contenuti;
- le liste di revoca e di sospensione ed i loro contenuti;
- la rappresentazione delle informazioni nelle buste PKCS#7.

La redazione delle Linee guida discende da un'analisi degli attuali standard internazionali e delle caratteristiche offerte dai prodotti di mercato.

Le tipologie di certificati cui si applicano le convenzioni stabilite nelle presenti Linee guida sono esclusivamente le seguenti:

1. certificati relativi a chiavi di certificazione di chiavi di sottoscrizione ai sensi del D.P.C.M. 8 febbraio 1999;
2. certificati relativi a chiavi di certificazione di chiavi di marcatura temporale ai sensi del D.P.C.M. 8 febbraio 1999;
3. certificati relativi a chiavi di sottoscrizione ai sensi del D.P.C.M. 8 febbraio 1999;
4. certificati relativi a chiavi di marcatura temporale ai sensi del D.P.C.M. 8 febbraio 1999.

Nessun certificato delle tipologie sopra indicate può essere utilizzato per scopo diverso da quello cui è destinato secondo la normativa.

Vengono presi in esame solo i formati di codifica, certificazione ed imbustamento delle firme utilizzate da tutti i certificatori finora iscritti nell'elenco pubblico, che sono rispettivamente il PKCS#1 (RSA), lo X.509 ed il PKCS#7 ver 1.5 (RFC 2315).

Per quanto attiene alle possibili differenze di formato, tutti i certificatori tratteranno le componenti di firma indistintamente nei formati ASN.1-DER (ISO 8824, 8825), BASE64 (RFC 1421) e PKCS#7 (RFC 2315).

Ciò significa che saranno elaborate correttamente tutte le componenti (certificato, busta PKCS#7, dati firmati, ecc.) indipendentemente da quale dei tre formati citati venga utilizzato per la trasmissione del dato.

Inoltre, si è convenuto che un ulteriore standard di riferimento dovesse essere il RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

2. Contenuti del certificato e loro rappresentazione

L'aderenza agli standard internazionali sulla certificazione delle chiavi pubbliche non è sufficiente a garantire la corretta rappresentazione delle informazioni relative all'identificazione del titolare.

In particolare, le varie possibilità offerte dagli standard in termini di rappresentazione dei dati e la loro realizzazione nei prodotti commerciali non garantiscono una completa interazione tra i vari prodotti.

Ulteriore difficoltà è la mancanza di una collocazione naturale per alcune tipologie di dati come il codice fiscale, che è di poco interesse in senso generale, ma ampiamente utilizzato (in verità è obbligatorio) nella pubblica amministrazione italiana.

Nell'intento di porre rimedio a questi problemi, si è stabilito che debbano essere inserite determinate informazioni – e con una certa struttura – in alcune componenti dell'identificativo del titolare (campo **subject**) nel certificato. Le componenti interessate (la cui presenza è quindi da considerarsi obbligatoria) sono:

- **common name** (object ID = 2.5.4.3);
- **description** (object ID = 2.5.4.13).

Di seguito si forniscono le regole per la valorizzazione e strutturazione delle due componenti.

a) Common Name = <cognome>/<nome>/<codice fiscale titolare>/<identificativo titolare presso il certificatore>.

Le parentesi acute individuano gli elementi non terminali. Il carattere / (slash) viene utilizzato come separatore di campo.

I quattro campi devono essere codificati usando il set di caratteri **PrintableString**.

Il campo <identificativo titolare presso il certificatore> contiene il dato di cui all'art. 11, comma 1, lettera c) del D.P.C.M. 8 febbraio 1999. Questo dato viene conservato nel COMMON NAME per garantire l'univocità del certificato e favorire eventuali operazioni di inserimento e ricerca all'interno del Directory X.500. Ai fini dell'interoperabilità, NON è importante identificare il meccanismo attraverso il quale il certificatore attribuisce questo dato, né la forma assunta dal medesimo.

Qualora uno stesso soggetto sia titolare di più certificati per più ruoli, deve possedere più codici identificativi distinti (come previsto dall'art. 22, comma 3 del D.P.C.M. 8 febbraio 1999).

Per quanto riguarda l'informazione relativa al ruolo del titolare, che permette di avere, per uno stesso soggetto, diversi certificati presso lo stesso certificatore (Art. 22, comma 3 del D.P.C.M. 8 febbraio 1999), questa può essere inserita nella DESCRIPTION (discusso di seguito).

Esempio: **CommonName** = "Rossi/Mario/RSSMRA60D02F220M/XYZ123456"

b) Description = "C=" <cognome esteso> "/N=" <nome esteso> "/D=" <data di nascita> ["/R=" <ruolo titolare>]

Il valore di description è quindi ottenuto dalla concatenazione di quattro campi "etichettati" (tagged), il cui ordine NON è rilevante. In grassetto sono evidenziate le etichette (tag) da utilizzare. Ai quattro campi si applicano le seguenti regole:

- <cognome esteso> è il cognome per esteso del titolare, eventualmente multiplo (es. "Battistotti Sassi");
- <nome esteso> è il nome per esteso del titolare, eventualmente multiplo (es. "Carlo Maria");
- la <data di nascita> deve essere rappresentata nel formato "GG-MM-AAAA" con il carattere "0" (zero) a completamento dei numeri ad una cifra;
- il <ruolo del titolare> è l'unico campo opzionale. Trattandosi di un dato di interesse applicativo e non determinante ai fini dell'interoperabilità, non si impongono regole nel suo formato.

La stringa risultante dalla concatenazione dei quattro campi può essere codificata col set di caratteri **BMPString** quando ciò è necessario per rendere in modo esatto l'ortografia originale del nome e cognome estesi del titolare (es. nel caso di nomi francesi, spagnoli, ecc.).

Es.: **description** = "C Großmann = /N= Günther/D=03-11-1947/R=Direttore Generale".

3. Estensioni del certificato e suoi contenuti

Le Linee guida prevedono che le estensioni che devono essere contenute nei certificati siano:

- Authority Key Identifier: seleziona una chiave tra quelle utilizzate dal Certificatore;
- Subject Key Identifier: seleziona una chiave tra quelle a disposizione del titolare;
- Key usage: indica l'uso delle chiavi;
- Extended Key Usage: fornisce indicazioni ulteriori sull'uso delle chiavi;
- Basic Constraints: specifica se la chiave corrispondente al certificato è una chiave di certificazione;
- Certificate Policies: specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo;
- CrIDistributionPoint: indica dove reperire la CRL;

La presenza e le caratteristiche di un'estensione dipendono dalla tipologia del certificato. La tabella che segue definisce, per i tre tipi di certificato considerati dalla normativa, le modalità di utilizzo di ciascuna estensione. Per l'interpretazione degli elementi si vedano le note esplicative appresso riportate

Estensioni X.509v3	Certificato per chiave di certificazione	Certificato per chiave di marcatura temporale	Certificato per chiave di sottoscrizione
Key Usage (15)	CRITICA KeyCertSign + cRLSign	CRITICA digitalSignature	CRITICA nonRepudiation
Basic Constraints (19)	CRITICA cA=true		
Extended Key Usage (37)		CRITICA keyPurposeId=ti meStamping	
Certificate Policies (32)	NON CRITICA PolicyIdentifier + URL del CPS	NON CRITICA policyIdentifier + URL del CPS	NON CRITICA policyIdentifier + URL del CPS
CRL Distribution Points (31)	NON CRITICA URL di accesso alla CRL/CSL		NON CRITICA URL di accesso alla CRL/CSL
Authority Key Identifier (35)		NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier
Subject Key Identifier (14)	NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier

Note esplicative:

- e. Ciascun elemento della tabella indica se l'estensione associata alla riga deve essere presente o meno nel certificato corrispondente alla colonna e, nel caso debba essere presente, quale valore deve assumere; nel caso in cui non si forniscano informazioni sul valore, si intende che questo deve essere impostato seguendo le indicazioni fornite nella specifica pubblica RFC 2459.
- f. Il numero riportato tra parentesi nella prima colonna accanto al nome dell'estensione è l'ultima parte dello OID che individua l'estensione stessa; tale numero segue il prefisso **{2 5 29}** che individua le estensioni di certificato (esempio: lo OID completo dell'estensione Key Usage è **{2 5 29 15}**).
- g. "CRITICA" significa che l'estensione **deve** essere presente nel certificato e marcata come critica.
- h. "NON CRITICA" significa che l'estensione **non deve** essere marcata come critica, ma tuttavia **deve** essere presente.
- i. Le celle ombreggiate indicano che la corrispondente estensione **non deve** essere presente nel certificato.
- j. TimeStamping = lo OID di valore **{1 3 6 1 5 5 7 3 8}** definito nella specifica pubblica RFC 2459.
- k. L'uso delle estensioni non indicate nella seguente tabella è a discrezione del certificatore, purché questi si attenga alla specifica pubblica RFC 2459.

4. Contenuti delle liste di revoca e sospensione

La rappresentazione delle liste di revoca e sospensione è identica, in quanto le liste di sospensione si possono considerare delle liste di revoca con il codice di revoca (CRLReason) di valore pari a 6 ("certificate hold"). Ad ogni emissione verrà prodotta un'unica lista contenente sia i certificati revocati, sia quelli sospesi.

Le liste di revoca e sospensione, emesse in formato X.509v2, oltre alle informazioni obbligatorie devono contenere le seguenti estensioni:

- estensioni al livello dell'intera lista: **cRLNumber** (il numero della CRL);
- estensioni a livello di singola entry: **reasonCode**.

Il valore di tale estensione, a livello di singola entry o di intera lista è a discrezione del certificatore, purché si seguano le regole fornite nella specifica pubblica RFC 2459.

5. Rappresentazione delle informazioni nelle buste PKCS#7

La struttura delle buste PKCS#7 deve essere aderente a quanto previsto nella specifica pubblica RFC 2315.

Le criticità individuate sono due:

- la rappresentazione dei dati interna ed esterna alla busta;
 - l'attributo autenticato "signing time".
- Per quanto concerne la rappresentazione dei dati, viene previsto quanto segue:
- il documento deve sempre essere *contenuto* nella busta crittografica (ovvero, non è ammessa la "detached signature");
 - il documento da firmare deve essere imbustato nel formato originale (senza header o trailer aggiuntivi);
 - il nome del file firmato (ossia della busta) deve assumere una doppia estensione in modo da conservare l'informazione relativa al tipo di documento che è stato firmato; il file firmato avrà quindi un nome del tipo: nome_file.tipo_documento_originale.P7M.

Il tipo documento deve seguire la prassi standard delle estensioni (".DOC" per i documenti MS Word™, ".PDF" per quelli Adobe Acrobat™, ".HTM" per la pagine web, ecc.). Eventuali collisioni che si venissero a determinare devono essere gestite a parte.

Per quanto concerne gli attributi autenticati, con le presenti Linee guida si stabilisce quanto segue.

L'attributo autenticato "signing time" si deve considerare opzionale, sia dal punto di vista della sua presenza/assenza nella busta PKCS#7, sia dal punto di vista dell'utilizzo del suo valore.

Per garantire l'interoperabilità nell'ambito della pubblica amministrazione, questo dato non può essere considerato critico. L'eventuale presenza di questo attributo autenticato (o di altri attributi autenticati) nella busta PKCS#7, quindi, non deve comportare di per sé l'accettazione piuttosto che il rifiuto della busta stessa. L'eventuale presenza di attributi autenticati sarà significativa solo in base a specifiche esigenze del particolare contesto applicativo in cui si opera, mentre non deve essere considerata significativa a livello di API crittografiche.

IL PRESIDENTE. REY

Riferimenti

Si riportano alcuni standard presi a riferimento per la stesura delle presenti Linee guida.

RFC 1421 (P.E.M.)

RFC 2437 (PKCS#1)

RFC 2459

RFC 2314 (PKCS#10)

RFC 2315 (PKCS#7)

X.501 - X.509 - X.520 - X.690 - X.691

ISO 10118-3 (Algoritmi di hash)

DECRETO DEL MINISTRO DELL'INTERNO 19 luglio 2000

Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici

(Gazz. Uff. 21 luglio 2000, n. 169, S.O.)

IL MINISTRO DELL'INTERNO

Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;

Visti il regio decreto 18 giugno 1931, n. 773 ed il regio decreto 6 maggio 1940, n. 635;

Vista la legge 31 dicembre 1996, n. 675;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

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

Sentita la Conferenza Stato-città ed autonomie locali, che ha espresso il proprio avviso nella riunione del 22 giugno 2000;

Decreta:

Capo I - Principi generali

1. Definizioni.

1. Ai sensi del presente decreto si intende:

a) per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

b) per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;

c) per «S.S.C.E.»: il sistema di sicurezza del circuito di emissione dei documenti;

d) per «S.A.I.A.»: il sistema predisposto dal Ministero dell'interno per l'accesso e l'interscambio anagrafico;

e) per «Istituto»: l'Istituto Poligrafico e Zecca dello Stato;

f) per «dati»: i dati identificativi della persona di cui all'art. 1, comma 1, lettera d) e gli altri elementi di cui all'art. 3, comma 1, lettere da b) ad h), del D.P.C.M.;

g) per «carta-servizi»: l'insieme dei dati di cui alla precedente lettera f) - ad esclusione della fotografia e della firma - e delle informazioni amministrative di cui all'art. 1, comma 1, lettera e) e dell'art. 3, comma 4, del D.P.C.M.;

h) per «codice cifrato»: la coppia di codici alfanumerici che identificano univocamente il microprocessore di ogni documento;

i) per «cartellino elettronico»: la trasposizione, in formato digitale e cifrata, del cartellino cartaceo di cui all'art. 290 del regio decreto 6 maggio 1940, n. 635;

j) per «P.I.N.»: il numero identificativo personale necessario alla fruizione dei servizi che ne richiedono l'utilizzo.

2. Funzioni dei comuni.

1. Le funzioni di pertinenza dei comuni possono essere esercitate anche in forma associata.

2. I comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato B al presente decreto, predispongono in piena autonomia i servizi locali.

3. Modalità di connessione.

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente e del D.P.C.M., esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica dei documenti

si connettono al S.S.C.E. con le modalità di cui all'allegato B e devono provvedere all'aggiornamento dell'indice delle anagrafi tramite collegamento al S.A.I.A.

4. Misure di sicurezza.

1. Ai fini della produzione, del rilascio, dell'aggiornamento e del rinnovo dei documenti, il trattamento dei dati, da parte delle amministrazioni e degli enti indicati dall'art. 3, comma 1, è effettuato nel rispetto dell'art. 15 della legge 31 dicembre 1996, n. 675 e delle disposizioni di cui al decreto del Presidente della Repubblica 28 luglio 1999, n. 318, nonché delle ulteriori prescrizioni tecniche descritte nell'allegato B.

5. Servizi e modalità di autenticazione.

1. Ai sensi dell'art. 3, comma 4, e dell'art. 7, comma 1, del D.P.C.M. tutti i servizi che non implicano la memorizzazione dei dati sui documenti sono predisposti in piena autonomia dalle amministrazioni. Le modalità di autenticazione in rete per l'accesso ai servizi da parte del titolare del documento sono definite nell'allegato B.

2. Per i servizi che richiedono la memorizzazione di dati sui documenti è necessaria l'installazione degli stessi da parte del comune e, qualora relativi a dati sensibili, la richiesta dell'interessato.

3. I servizi nazionali che richiedono la memorizzazione di dati sui documenti sono predisposti con le modalità e nel rispetto delle regole tecniche di cui all'allegato B.

Capo II - Regole tecniche di base

6. S.S.C.E. e software di sicurezza.

1. In attuazione dell'art. 8, commi 1 e 4, del D.P.C.M. il Ministero dell'interno - Dipartimento della pubblica sicurezza, mette a disposizione delle questure e dei comuni l'infrastruttura organizzativa, informatica e di rete del Centro elaborazioni dati della Polizia scientifica per la realizzazione, la gestione e la manutenzione del S.S.C.E., nonché fornisce ai comuni un software di sicurezza finalizzato a garantire l'integrità, l'accessibilità e la riservatezza delle informazioni nelle fasi di compilazione, rilascio, aggiornamento, rinnovo e verifica dei documenti.

2. Ai sensi dell'art. 6, comma 1, del D.P.C.M. le questure, nei casi previsti dallo stesso articolo, procedono all'interdizione dell'operatività del documento secondo le modalità descritte nell'allegato B.

3. Le questure, ai sensi dell'art. 290 del regio decreto 6 maggio 1940, n. 635, conservano il cartellino elettronico, a cui accedono in via esclusiva, relativo ai documenti rilasciati dai comuni della stessa provincia.

7. Supporto fisico.

1. Il supporto fisico del documento è costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato dai supporti informatici di cui all'art. 8.

2. Il supporto fisico è stampato con le tecniche tipiche della produzione di carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento visivamente e mediante strumenti portatili e di laboratorio.

3. Il documento ha le caratteristiche grafiche di cui al modello approvato con il presente decreto e di cui all'allegato A.

8. Supporti informatici.

1. Il supporto fisico di cui all'art. 7 è dotato di una banda ottica per la memorizzazione, con modalità informatiche di sicurezza, dei dati riportati graficamente sul documento, nonché

di un microprocessore per la memorizzazione della carta-servizi e per le operazioni connesse alle procedure di identificazione in rete del titolare del documento. Gli standard internazionali, le caratteristiche tecniche e l'architettura logica dei predetti supporti informatici sono conformi alle specifiche indicate nell'allegato B.

9. Inizializzazione del documento.

1. L'Istituto, cui è riservata la produzione dei documenti a norma dell'art. 11 del presente decreto, provvede alla inizializzazione delle componenti fisiche ed informatiche del documento secondo le procedure di sicurezza descritte nell'allegato B. A seguito della inizializzazione il documento acquisisce la qualità di documento in bianco.

10. Configurazione hardware e software per la formazione del documento.

1. Ai fini della formazione dei documenti, i comuni utilizzano la configurazione hardware descritta nell'allegato B.

2. Ai fini della compilazione, rilascio, aggiornamento e rinnovo dei documenti i comuni utilizzano il software di sicurezza di cui all'art. 6, comma 1.

Capo III - Norme procedimentali

11. Produzione del documento.

1. La produzione del documento è riservata all'Istituto che vi provvede ottemperando alle norme che disciplinano la produzione delle carte valori e dei documenti di sicurezza della Repubblica italiana e agli standard internazionali di sicurezza previsti per l'emissione di carte di pagamento.

2. Nella fase di produzione a regime dei documenti elettronici di cui al presente decreto, l'Istituto, nell'ambito di proprio stabilimento, costituisce uno speciale settore con accesso limitato ai dipendenti addetti alle specifiche lavorazioni e sorvegliato dalle Forze di polizia, dotato altresì delle sicurezze fisiche anti-effrazione e dei sistemi di sorveglianza elettronici definiti di intesa con il Ministero dell'interno.

12. Trasmissione del documento in bianco in periferia e sua custodia da parte del comune.

1. La trasmissione alle prefetture dei documenti in bianco è effettuata dal Provveditorato generale dello Stato, d'intesa con l'Istituto, in condizioni di sicurezza, mediante affidamento dei plichi a vettori specializzati nel trasporto di valori.

2. Il comune adotta ogni idonea misura per la custodia dei documenti in bianco in condizioni di sicurezza.

13. Procedura di sicurezza per la formazione e rilascio del documento.

1. La formazione ed il rilascio del documento avvengono nel rispetto della seguente procedura di sicurezza:

a) il comune, utilizzando le funzionalità del software di sicurezza di cui all'art. 10, comma 2, genera un messaggio informatico cifrato, costituito dai dati del richiedente e dal codice cifrato necessario all'identificazione in rete del documento e lo invia telematicamente al S.S.C.E.;

b) i dati, ad eccezione del codice fiscale e del numero identificativo del documento, vengono registrati cifrati dal S.S.C.E.; l'accesso ai predetti dati in chiaro è consentito esclusivamente alla questura territorialmente competente;

c) il comune, ricevuta la necessaria abilitazione ad emettere il documento da parte di S.S.C.E., riporta i dati identificativi della persona sul microprocessore e sulla banda ottica secondo le modalità indicate nell'allegato B ed effettua la stampa di tali dati sul supporto fisico;

d) il comune genera il P.I.N., lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione e lo consegna, insieme al documento, al titolare.

2. In via transitoria, i comuni possono avvalersi dell'Istituto ai fini della formazione del documento, utilizzando una configurazione hardware conforme ad uno standard minimo corrispondente alle dotazioni descritte nell'allegato B. In tali casi il software di sicurezza provvede ad inoltrare all'Istituto il messaggio informatico di cui al comma 1, lettera a). L'Istituto non conserva traccia dei dati utilizzati per la formazione del documento.

3. L'Istituto assicura livelli di servizio che consentono la disponibilità presso le prefetture dei documenti formati entro il termine di venti giorni successivi alla ricezione del messaggio informatico di cui al comma 2.

Capo IV - Sperimentazione

14. Avvio della fase di sperimentazione.

1. I comuni che intendono partecipare alla fase di sperimentazione prevista dall'art. 9 del D.P.C.M. presentano il relativo progetto al Ministero dell'interno.

2. I progetti di cui al comma 1 devono contenere:

a) l'indicazione della data di inizio e della durata della sperimentazione e del responsabile del progetto;

b) la descrizione delle modalità organizzative in rapporto alla dimensione territoriale della sperimentazione e alla stima del quantitativo, effettuata su base presuntiva, dei documenti da rilasciare nel periodo di sperimentazione;

c) la descrizione delle procedure di gestione e dei flussi di dati con specifico riferimento alle modalità di connessione di cui all'art. 3, la descrizione delle procedure di sicurezza, la descrizione delle procedure di controllo;

d) l'analisi dei rischi e la descrizione delle relative contromisure, con specifico riferimento a quelle destinate a prevenire la perdita accidentale delle informazioni trattate;

e) l'indicazione dei servizi da erogare relativamente alla carta-servizi.

3. La sperimentazione è autorizzata ai sensi dell'art. 9 del D.P.C.M. in relazione al numero di carte disponibili, tenendo conto dell'ordine cronologico di presentazione dei progetti di sperimentazione.

4. Il Ministero dell'interno può chiedere che il progetto di sperimentazione venga modificato o integrato. In tal caso si applica la disposizione dell'art. 9, comma 3, secondo periodo, del D.P.C.M.

15. Relazione sullo stato della sperimentazione.

1. Il responsabile del progetto trasmette, con cadenza bimestrale, al Ministero dell'interno relazioni sullo stato di avanzamento della sperimentazione.

2. Il Ministero dell'interno trasmette copia del progetto di sperimentazione e delle relazioni sullo stato di avanzamento della sperimentazione al Comitato di monitoraggio previsto dall'art. 10 del D.P.C.M.

Allegato B
Indice dei contenuti

1. INTRODUZIONE
- 1.1 BIBLIOGRAFIA DI RIFERIMENTO E STANDARD UTILIZZATI
- 1.2 STRUTTURA DELLA CARTA
2. INFRASTRUTTURA ORGANIZZATIVA (FA RIFERIMENTO ALL'ART. 3 DEL D.M.)
3. INFRASTRUTTURE TECNICHE E DI RETE
- 3.1 DOTAZIONI DEL SSCE (FA RIFERIMENTO ALL'ART. 6 DEL D.M.)
- 3.2 DOTAZIONI DEI COMUNI
- 3.2.1 Dotazioni hardware (fa riferimento all'art. 10 comma 1 del D.M.)
- 3.2.2 Dotazioni hardware minimale (fa riferimento all'art. 13 comma 2 del D.M.)
- 3.2.3 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)
- 3.2.4 Modalità di connessione al Sistema di Sicurezza del Circuito di Emissione (SSCE)
4. MATERIALI E STANDARD DI RIFERIMENTO
- 4.1 SUPPORTO FISICO (FA RIFERIMENTO ALL'ART. 7, COMMA 1 DEL D.M.)
- 4.1.1 Dimensioni nominali e le componenti
- 4.2 CARTA A MEMORIA OTTICA (FA RIFERIMENTO ALL'ART. 8, COMMA 1 DEL D.M.)
- 4.3 MICROPROCESSORE (FA RIFERIMENTO ALL'ART. 8, COMMA 1 DEL D.M.)
- 4.4 DATI (FA RIFERIMENTO ALL'ART. 13, COMMA 1, LETTERA D DEL D.M.)
5. MISURE DI SICUREZZA (FA RIFERIMENTO ALL'ART. 4 DEL D.M.)
- 5.1 SICUREZZA DEL SUPPORTO FISICO
- 5.1.1 Elementi di sicurezza grafici e di stampa
- 5.1.2 Inchiostri
- 5.1.3 Numerazione di serie
- 5.1.4 Applicazione di elementi Optical Variable Device (OVD)
- 5.2 SICUREZZA DELLA FASE DI PERSONALIZZAZIONE
- 5.3 AFFIDABILITÀ DEI DATI
- 5.3.1 Laser su banda ottica
- 5.3.2 Microcircuito
- 5.4 SICUREZZA DEL CIRCUITO (FA RIFERIMENTO ALL'ART. 6, COMMA 1 DEL D.M.)
- 5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)
- 5.4.2 Sicurezza della carta
- 5.4.3 Furto della carta «attivata» o documento in bianco
- 5.4.4 Controlli a vista
- 5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6 comma 2 del D.M.)
- 5.4.6 Software di sicurezza distribuito ai comuni (fa riferimento all'art. 6 comma 1 del D.M.)
6. SERVIZI EROGABILI IN RETE (FA RIFERIMENTO ALL'ART. 5 DEL D.M.)
- 6.1 LE LISTE DEI SERVIZI E LA LISTA DELLE CARTE INTERDETTE (BLACK-LIST)
- 6.2 MODALITÀ DI RICONOSCIMENTO IN RETE
- 6.2.1 Crypto Middleware ed API PKCS#11
- 6.2.2 Processo di Strong Authentication
- 6.2.3 Comandi di gestione utilizzati dalla Strong Authentication
- 6.3 CONSIDERAZIONI SULLA INTEROPERABILITÀ
- 6.3.1 Algoritmi
- 6.3.2 Formati
- 6.4 STRONG AUTHENTICATION LATO SERVER
- 6.4.1 Server Authentication Middleware
- 6.5 L'INSTALLAZIONE DEI SERVIZI

- 6.6 L'AGGIORNAMENTO DEI DATI RELATIVI ALLA FRUIZIONE DEI SERVIZI
- 6.7 AUTENTICAZIONE ESTERNA
- 6.8 SECURE MESSAGING
- 7. PROCESSO DI EMISSIONE
 - 7.1 PRODUZIONE DI BANDA LASER E MICROPROCESSORE
 - 7.2 PRODUZIONE ED INIZIALIZZAZIONE DELLA CARTA D'IDENTITÀ ELETTRONICA E DEL DOCUMENTO ELETTRONICO
 - 7.2.1 Struttura delle informazioni sulla banda ottica
 - 7.2.2 Struttura delle informazioni nel microprocessore
 - 7.3 LE FASI PRELIMINARI
 - 7.3.1 Generazione numeri identificativi per le carte d identità ed i documenti elettronici.
 - 7.3.2 Produzione
 - 7.3.3 Inizializzazione
 - 7.3.4 Attivazione
 - 7.4 PERSONALIZZAZIONE ED EMISSIONE DELLE CARTE
 - 7.4.1 Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)
 - 7.4.1.1 Sottofase di compilazione
 - 7.4.1.2 Sottofase di autorizzazione
 - 7.4.1.3 Sottofase di formazione
 - 7.4.1.4 Sottofase di rilascio
 - 7.4.1.5 Sottofase di verifica e controllo
- 8. VERIFICA DELLE CIE (FA RIFERIMENTO ALL'ART. 6, COMMA 1 DEL D.M.)
 - 8.1 CONSERVAZIONE DEL CARTELLINO ELETTRONICO (FA RIFERIMENTO ALL'ART. 6, COMMA 3 DEL D.M.)
 - 8.2 INTERDIZIONE DELL'OPERATIVITÀ DELLA CIE (FA RIFERIMENTO ALL'ART. 6, COMMA 2 DEL D.M.)

1. Introduzione

1.1 Bibliografia di riferimento e standard utilizzati

- Schema per il circuito di emissione della Carta di Identità elettronica, Roma 22 dicembre 1999 - AIPA/Associazioni dei fornitori - Gruppo di lavoro Carta d'Identità Elettronica;
- Processo di autenticazione in rete. Roma 22 dicembre 1999 - AIPA/Associazioni dei fornitori - Gruppo di lavoro Carta d'Identità Elettronica;
- CCITT X 208 per le Abstract Syntax Notation One (ASN.1);
- CCITT X 209 per le Basic Encoding Rules (BER) della sintassi ASN.1;
- RSA Laboratories Technical Notes: A Layman's Guide to a Subset of ASN. 1, BER and DER (Distinguished Encoding Rules);
- CCITT X 509 versione 3 per il formato dei Certificati Digitali, le estensioni e le policy;
- 2 FIPS 180-1 per la funzione di Hash SHA-1;
- FIPS 46 per il Data Encryption Standard;
- RSA 78 Rivest, Shamir, Aldeman. A method for obtaining digital signatures and public key Cryptosystems;
- PKCS#1 per il formato dei dati da sottoporre ad autenticazione;
- PKCS#7 per la sintassi dei dati da sottoporre ad autenticazione;
- PKCS#9 per i «selected attribute type» da utilizzare nella sintassi PKCS#7 e PKCS#10;
- PKCS#10 per la sintassi delle richieste di certificazione di chiavi pubbliche;
- ISO/IEC 11694-1-2-3-4 Annex A e Annex B per la parte relativa alla banda ottica;
- ISO/IEC 7816-1-2-3-4-5-6-7-8-9 per la parte relativa al microchip.

1.2 Struttura della carta

La carta d'identità elettronica (CIE) è una carta ibrida, in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore.

La banda ottica a lettura laser è utilizzata per la memorizzazione dei «dati» identificativi (D.M. Art. 1, comma 1, lettera f)) ai fini della salvaguardia delle esigenze di pubblica sicurezza. L'elevata capacità di memoria disponibile, utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità elaborativa del microchip, può consentirne un utilizzo anche per la fruizione di servizi locali o nazionali.

Il microprocessore è utilizzato per assolvere le funzioni di «carta servizi» (D.M. Art. 1, comma 1, lettera g)), per consentire l'identificazione in rete e, quindi, l'erogazione di servizi telematici.

Le caratteristiche grafiche della CIE (D.M. art. 7 comma 3), unitamente al dettaglio delle informazioni presenti, sono riportate nell'allegato A.

2. Infrastruttura organizzativa (fa riferimento all'art. 3 del D.M.)

Nel circuito di emissione intervengono gli enti nel seguito descritti:

Fornitori di microprocessori: Aziende produttrici dei microprocessori.

Provvedono alla fornitura dei microprocessori, durante la produzione memorizzano, in area non riscrivibile, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di chip, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di microprocessori consegnati ed i relativi numeri seriali impressi al loro interno.

Acronimo Fp

Fornitori di bande laser: Aziende produttrici della banda ottica a lettura laser.

Provvedono alla fornitura delle bande ottiche a lettura laser durante il processo di produzione imprimono, tramite scrittura laser, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di bande ottiche, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di bande ottiche consegnate ed i numeri seriali impressi al loro interno.

Acronimo Fb

Istituto Poligrafico e Zecca dello Stato: Ente a cui è riservata la produzione del documento.

Provvede alla manifattura delle carte, all'inserimento (embedding) della banda ottica e del microprocessore nel supporto fisico, nonché alla inizializzazione elettrica di quest'ultimo.

Memorizza nel chip, ai fini della garanzia di autenticità, nella banda ottica tramite laser e nella banda ottica in modalità «Embedded hologram» il numero d'identificazione univoco su scala nazionale, fornitogli dal Sistema di Sicurezza del Circuito di Emissione, ed inscindibilmente legato ad essa.

Imprime lo stesso numero in maniera grafica sul supporto fisico e stampa gli elementi grafici costanti (logo, sfondo, etc.).

Contabilizza i numeri seriali che identificano il lotto e la data di produzione del chip e della banda ottica.

Trasmette le informazioni risultanti dalle procedure di inizializzazione al Sistema di Sicurezza.

Acronimo IPZS

Ministero dell'Interno Sistema di Sicurezza del Circuito di Emissione: Ente che fornisce le infrastrutture tecnologiche e garantisce la sicurezza dell'intero circuito di emissione.

In attuazione dell'art. 8, comma 4, del D.P.C.M. 22 ottobre 1999, n. 437, il Ministero dell'Interno - Dipartimento della Pubblica sicurezza mette a disposizione l'infrastruttura organizzativa, informatica di rete del Centro Elaborazioni Dati della Polizia Scientifica, per la realizzazione, la gestione e manutenzione del Sistema di sicurezza del circuito di emissione.

Al fine di garantire la sicurezza dell'intero circuito di emissione ha la responsabilità di verificare e certificare qualunque operazione che comporti l'inserimento, la modifica o la cancellazione delle informazioni (in particolare i dati identificativi) memorizzate sul microprocessore o sulla banda ottica, eccezion fatta per i dati relativi alla predisposizione ed erogazione dei servizi.

Ai fini della garanzia di autenticità, genera per ogni carta un numero di identificazione univoco, su scala nazionale, che trasmette all'IPZS.

Tramite collegamenti telematici consente alle singole Questure di accedere ai documenti, conservati in forma cifrata presso il sistema.

Ciascuna Questura, e solo essa, può decrittare i documenti di sua competenza, ovvero quelli rilasciati dai Comuni della stessa Provincia.

Acronimo SSCE

Ministero dell'Interno SAIA: Sistema di Accesso e Interscambio Anagrafico.

Sistema di interscambio dati anagrafici tra le procedure informatiche delle diverse Amministrazioni Pubbliche per fornire servizi integrati al cittadino focalizzando sul Comune la registrazione di tutti gli eventi che comportano un aggiornamento delle informazioni anagrafiche riportate nelle diverse banche dati settoriali della P.A.

Acronimo SAIA

Emittitore: Ente responsabile della formazione e del rilascio.

È il Comune al quale il cittadino si rivolge per richiedere la CIE.

Acronimo E

3. Infrastrutture tecniche e di rete

3.1 Dotazioni del SSCE (fa riferimento all'art. 6 del D.M.)

Ai fini dell'emissione della CIE, il sistema di sicurezza del circuito d'emissione (SSCE) si compone di:

- connessione alle reti di accesso;
- funzioni di «security service provider» per consentire l'accesso, con modalità di sicurezza, dei Comuni tramite Internet;
- rete digitale delle Questure (già presente) per consentire la visualizzazione e la stampa dei Cartellini Elettronici alle Questure competenti;
- connessione diretta con l'IPZS per l'interscambio d'informazioni nella fase d'inizializzazione;
- software di sicurezza versione server per le funzionalità connesse alle diverse fasi di formazione della CIE.

3.2 Dotazioni dei Comuni

3.2.1 Dotazioni hardware (fa riferimento all'art. 10, comma 1 del D.M.)

Nel seguito è riportata la configurazione di massima degli apparati hardware necessari per la formazione della CIE. Le apparecchiature proposte possono subire variazioni in funzione dell'architettura del sistema informativo dei singoli comuni.

- 1) Personal Computer di fascia alta;
- 2) Stampante ad impatto per l'impressione del PIN sulla carta chimica retinata;
- 3) Lettore/scrittore di banda ottica. Il lettore deve essere provvisto anche di un lettore di microprocessore, al fine di evitare problemi di allineamento delle informazioni.
- 4) Lettore scrittore di microprocessore;
- 5) Stampante termografica per l'impressione sul supporto fisico dei dati del titolare. Anche la stampante termografica deve essere provvista di lettore di microprocessore;
- 6) Scanner per la digitalizzazione della firma e, eventualmente, della fotografia del titolare;
- 7) Videocamera per la produzione digitalizzata della fotografia del titolare;
- 8) Scanner per l'assunzione delle impronte digitali. Lo scanner deve acquisire ad una risoluzione di 500 dpi;
- 9) Apparecchiatura per l'applicazione sul fronte del documento, di un «overlay» di sicurezza.

3.2.2 Dotazioni hardware minimale (fa riferimento all'art. 13, comma 2 del D.M.)

Nel seguito è riportata la configurazione minima degli apparati hardware necessari per la formazione della CIE in caso il comune si avvalga, in via transitoria, dell'IPZS. Le apparecchiature proposte possono subire variazioni in funzione dell'architettura del sistema informativo dei singoli comuni.

- 1) Personal Computer di fascia alta;
- 2) Scanner per la digitalizzazione della firma e, eventualmente, della fotografia del titolare;
- 3) Videocamera per la produzione digitalizzata della fotografia del titolare;
- 4) Scanner per l'assunzione delle impronte digitali. Lo scanner deve acquisire ad una risoluzione di 500 dpi;

3.2.3 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)

I comuni, per le attività inerenti la formazione ed il rilascio delle CIE, saranno dotati di specifico software applicativo di sicurezza, sviluppato e distribuito da SSCE.

Tale software avrà la possibilità di interoperare con i sistemi informativi dei comuni.

3.2.4 Modalità di connessione al Sistema di Sicurezza del Circuito di Emissione (SSCE)

L'interconnessione a SSCE avverrà secondo le seguenti modalità di trasporto:

- tramite rete unitaria della Pubblica Amministrazione (RUPA);
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite internet.

In tutti i casi è necessario l'utilizzo del software di sicurezza versione client.

Il software consente di eseguire le funzioni necessarie per l'acquisizione dei dati del titolare, utili alla formazione del documento, e quelle per operare, con modalità di sicurezza, le connessioni a SSCE.

4. Materiali e standard di riferimento

4.1 Supporto fisico (fa riferimento all'art. 7, comma 1 del D.M.)

4.1.1 Dimensioni nominali e le componenti

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO)/IEC 7816-1, 7816-2.

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 1995 per la carta di tipo ID-I. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore della CIE, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

La CIE, sarà costituita da materiali plastici compatibili con gli strumenti tecnologici in essa contenuti, nonché con i sistemi di personalizzazione utilizzati per la sua compilazione.

La CIE, per un uso normale nel periodo di validità, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 1995 relativamente a: deformazioni, tossicità, resistenza ad agenti chimici, stabilità dimensionale ed inarcamento con temperatura e umidità, inarcamento con l'uso, infiammabilità e durata.

- nella norma ISO/IEC 11693 per la contaminazione, per la trasmissione della luce attraverso lo spessore della carta e per la resistenza agli agenti atmosferici ed ai test di compatibilità con l'ambiente.

Per quanto attiene alla presenza del microchip la CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816 - 1.

L'area a memoria ottica della CIE, per un normale uso durante il periodo di validità, deve rispondere alle specifiche definite dalle norme ISO/IEC 11693, 11694-1, 11694-2, 11694-3, 11694-4.

4.2 Carta a memoria ottica (fa riferimento all'art. 8, comma 1 del D.M.)

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, 1.000 volte più resistente del PVC, che garantisce un'ottima trasparenza per la scrittura su banda ottica, una elevata resistenza, una maggiore durata nel tempo ed un intervallo termico di utilizzo molto ampio (-40° + 100°).

Il film è composto da diversi strati di materiale ed il supporto ottico registrabile è incapsulato tra due livelli di materiale protettivo trasparente che (sulla faccia esterna) è rinforzato da un ulteriore strato «antigraffio».

La capacità di memoria della carta ottica utilizzata, nella dimensione adottata, è di circa 1,8 MByte.

Ogni carta ottica permette la creazione di settori variabili basati su tracce, consentendo così l'archiviazione di informazioni multiple ed indipendenti.

Le carte ottiche, rispondono allo standard ISO/IEC 11694.

4.3 Microprocessore (fa riferimento all'art. 8, comma 1 del D.M.)

È composto da un circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, e da un circuito integrato (chip) incastonati sulla scheda.

La capacità di elaborazione propria del microcircuito (chip) che lo distingue da qualunque altro supporto «passivo», permette di classificare la CIE come una «smart card» (carta intelligente).

La presenza di un vero sistema operativo e di una memoria riscrivibile e non volatile (EEPROM) rende possibile proteggere i dati memorizzati ed eseguire istruzioni e programmi, in modo del tutto simile ad un vero computer.

La caratteristica, propria del microcircuito, di poter nascondere informazioni all'esterno di esso, ed al contempo di poter eseguire istruzioni o programmi interni, rende possibile il riconoscimento sicuro della carta per via telematica e la conseguente ed immediata erogazione dei servizi.

In particolare, la presenza del microcircuito sulla carta d'identità elettronica rende possibili:

- l'identificazione sicura, per via telematica, della carta (e del suo titolare) da parte di un server remoto, sede di un servizio erogato;
- l'identificazione, per via telematica, del servizio remoto da parte della carta (il titolare della carta deve essere sicuro che il servizio cui accede - senza poterlo «fisicamente» vedere - sia autentico, altrimenti potrebbe esporre i dati sensibili, memorizzati sulla carta, a lettura non autorizzata o addirittura a contraffazione non rilevata);
- la possibilità di stabilire un canale sicuro di comunicazione tra la CIE ed il server remoto attraverso la cifratura delle informazioni. Il canale cifrato deve quindi «attraversare» l'applicazione client (ad es. il browser) utilizzata per accedere al servizio, al fine di evitare la possibilità di un «attacco nel mezzo».

La capacità di memoria del microcircuito, in larga parte offerta dalla sua memoria riscrivibile e non volatile (EEPROM), varia attualmente da 2 a 32 Kb con una rapida evoluzione a 64 Kb.

Per la CIE, è richiesta una memoria EEPROM dalla capacità non inferiore a 16 Kb.

Un'altra caratteristica del microcircuito è la presenza di un coprocessore crittografico, che rende estremamente veloci le operazioni di cifratura e di decifratura. Il motore crittografico presente sulla CIE è in grado di eseguire, in modalità nativa, almeno l'operazione di RSA signature con chiavi non inferiori a 1024 bit.

Il circuito stampato, che protegge il chip dallo sforzo meccanico e dall'elettricità statica, deve essere conforme alla norma ISO 7816-3 che fornisce cinque punti di collegamento per potenza e dati.

Gli standard di riferimento, per il microcircuito e per i comandi del sistema operativo da esso ospitato, sono i seguenti:

- ISO 7816-3
- ISO 7816-4
- ISO 7816-8

I comandi, nella forma di APDU, che devono obbligatoriamente rispettare gli standard citati, sono quelli utilizzati dal middleware crittografico di interfaccia con la carta, le cui specifiche sono discusse nel paragrafo che descrivere il processo di autenticazione in rete.

Fa eccezione il comando per lo scambio delle chiavi di sessione, descritto nella sezione riguardante i servizi, che dovrà essere implementato secondo le specifiche riportate in quel paragrafo.

4.4 Dati (fa riferimento all'art. 13, comma 1, lettera d) del D.M.)

Di seguito è riportato il formato elettronico dei dati presenti nella CIE.

La dimensione dei vari campi, indicati nella tabella, sarà definita a seguito della elaborazione delle specifiche di dettaglio.

5. Misure di sicurezza (fa riferimento all'art. 4 del D.M.)

Questo paragrafo descrive le misure adottate, durante tutte le fasi della produzione e dell'utilizzo della CIE, per ottenere i corretti livelli di sicurezza e di interoperabilità della carta.

5.1 Sicurezza del supporto fisico

Nel seguito sono elencati gli elementi utilizzabili per la sicurezza del supporto e per accertarne l'autenticità, anche attraverso il semplice esame visivo.

5.1.1 Elementi di sicurezza grafici e di stampa

È previsto l'uso dei seguenti elementi di sicurezza, tipici delle carte valori:

- motivi antiscanner ed antifotocopiatura a colori;
- stampa con effetto rainbow (a sfumatura di colore graduale e progressiva);
- motivi grafici multicolore richiedenti elevata qualità di registro di stampa;
- microprint;
- processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico;
- embedded hologram (incisione grafica su banda laser);

5.1.2 Inchiostri

Per la stampa è previsto l'impiego di inchiostri dotati di speciali caratteristiche, come quelli fluorescenti (visibili all'ultravioletto), interferenziali e otticamente variabili (OVI - Optical Variable Ink).

5.1.3 Numerazione di serie

La numerazione del documento in bianco, realizzata con sistema ad incisione laser sul fronte del documento, è ripetuta visibilmente sulla banda ottica con il sistema dell'«embedded Hologram», memorizzata al suo interno ed inserita come dato all'interno del microprocessore.

5.1.4 Applicazione di elementi Optical Variable Device (OVD)

Sul retro del documento, nella fase di produzione, è applicato a caldo un ologramma di sicurezza.

Sul fronte del documento, quale ultima fase della personalizzazione, è prevista l'applicazione di overlay olografico.

5.2 Sicurezza della fase di personalizzazione

Al fine di consentire la stampa della CIE presso i Comuni o i Centri Servizi ad un costo contenuto, la tecnica da utilizzare è quella della termografia a colori su policarbonato (eventualmente apponendo uno strato neutro intermedio).

Anche la compilazione grafica sarà uniforme per tutto il territorio nazionale tramite l'utilizzo di caratteri, provenienti da un unico «font» appositamente realizzato per la CIE che verrà distribuito unitamente al software di sicurezza, dal SSCE.

Inoltre, l'apposizione di embedded hologram (incisione grafica su banda laser) consente di replicare, su banda ottica, i dati identificativi del titolare del documento, al fine di rendere più sicura l'identificazione a vista.

Infine, come accennato, al termine della stampa termica, il processo prevede l'applicazione sul fronte di un «overlay» di protezione di 12 micron al fine di offrire ulteriori sicurezze e garantire la durata oltre i cinque anni.

5.3 Affidabilità dei dati

5.3.1 Laser su banda ottica

I dati vengono memorizzati permanentemente sulla banda laser (sistema WORM) in formato digitale e letti/scritti con appositi apparati, detti lettori/scrittori.

Ferma restando l'auspicabile corretta conservazione da parte del titolare della carta, per meglio garantire la leggibilità e la coerenza dei dati nel tempo, la superficie della tessera dovrebbe presentarsi pulita e uniforme (es. possibilmente senza graffi o abrasioni). Comunque i supporti informatici utilizzati offrono garanzie di conservazione dei dati molto elevate; infatti, per quanto attiene ai dati contenuti nella banda laser, è attivo un metodo di identificazione e correzione d'errore che garantisce la ricostruzione delle informazioni digitali eventualmente perse per cause accidentali.

5.3.2 Microcircuito

Esistono due distinti livelli di protezione dei dati conservati nella carta: un livello fisico ed un livello logico. La protezione a livello fisico è gestita dal produttore del chip che provvede a mascherare sulla carta, in maniera indelebile, il sistema operativo proteggendolo mediante una chiave segreta di cui egli solo è a conoscenza.

Il livello logico è invece gestito sia dall'entità che inizializza la CIE che dall'ente che la personalizza.

Tre sono le tipologie di dati che il microcircuito contiene

- le informazioni specifiche dell'hw e del sw
- le informazioni anagrafiche del titolare,
- i dati relativi alla carta servizi, cioè necessari alla fruizione dei servizi erogati da un server remoto.

Per quanto riguarda la prima e la seconda tipologia di dati la registrazione può avvenire soltanto dopo il superamento di particolari condizioni di test e, una volta effettuata, comporta l'aggiornamento dei diritti di accesso ai dati, al fine di impedirne una successiva cancellazione o modifica.

Relativamente alla terza tipologia i dati possono essere distinti in:

- dati individuali aggiuntivi- dati relativi ai singoli servizi.

L'accesso a questi ultimi dati è possibile solo dopo il consenso del titolare espresso ordinariamente tramite digitazione di PIN.

I dati individuali aggiuntivi sono informazioni relative al titolare che sono registrate sulla carta, ad integrazione delle informazioni anagrafiche, e che possono essere utilizzate ai fini dell'erogazione dei servizi. Queste informazioni estendono l'identità del titolare, non sono specifiche di un servizio e non sono modificabili a seguito dell'erogazione dei servizi. Vengono registrate o modificate sulla carta esclusivamente dal Comune su esplicita richiesta del titolare e, in pratica, abilitano la carta all'accesso a quei servizi delle amministrazioni locali e centrali la cui erogazione necessita di tali dati.

L'elenco dei dati individuali aggiuntivi è definito ed aggiornato dal Dipartimento della Funzione Pubblica, d'intesa con il Ministero dell'Interno e con l'Associazione Nazionale dei Comuni d'Italia.

I dati relativi ai singoli servizi sono informazioni registrate sulla carta, eventualmente modificabili durante l'erogazione del servizio, e relative ad attributi del titolare della carta che sono funzionali esclusivamente all'amministrazione erogante il servizio.

5.4 Sicurezza del circuito (fa riferimento all'art. 6, comma 1 del D.M.)

La migliore garanzia contro tentativi di falsificazioni e utilizzo di carte rubate si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione della CIE.

In tale logica, il sistema di sicurezza dei documenti traccia tutte le operazioni al fine di garantire il rispetto della normativa vigente sulla riservatezza delle informazioni e dei dati personali, per impedire l'emissione di documenti falsi e per individuare facilmente l'utilizzo fraudolento di documenti rubati e la contraffazione di documenti autentici.

Nel capitolo 7 verranno descritte dettagliatamente tutte le fasi del processo di emissione.

5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)

In base al Regolamento di esecuzione del Testo Unico delle Leggi di P.S., oltre al titolare possono accedere alle informazioni contenute nei documenti esclusivamente i Comuni, che emettono le carte d'identità, e le Questure competenti territorialmente. Infatti, sia gli uni che gli altri sono tenuti a conservare copia dei documenti emessi.

Passando da un documento cartaceo ad uno di formato elettronico, anche la copia conservata da Comune e Questura (cartellino cartaceo) diviene di tipo digitale (cartellino elettronico).

Pertanto, a fini di sicurezza e nel rispetto delle norme di legge, la «base dati» comune consente l'accesso e la visualizzazione dei cartellini elettronici al solo Comune di residenza ed alla Questura territorialmente competente.

A tal fine il Sistema di Sicurezza (SSCE) garantisce la tracciabilità di tutte le attività, relative ai dati identificativi, per ogni singolo documento, consentendo di risalire, in qualsiasi momento, alle informazioni di «chi ha fatto cosa e quando», nel rispetto delle attuale normativa, durante tutte le fasi di formazione, compilazione, rilascio, rinnovo ed aggiornamento dei documenti.

Il Sistema di Sicurezza, grazie ad un meccanismo di cifratura basata su algoritmo a chiave asimmetrica, non è in grado esso stesso di accedere ad alcuna informazione di carattere personale che può essere visualizzata, tramite la propria chiave privata, esclusivamente dalla Questura o dal Comune competente.

Da un punto di vista tecnico, i dati sono prima cifrati per mezzo di un algoritmo simmetrico di provata robustezza (ad es. 3DES) con una chiave di lunghezza non inferiore a 128 bit (generata in modalità casuale); quest'ultima, prima di essere distrutta, viene a sua volta cifrata sia con la chiave pubblica della Questura che con quella del Comune e memorizzata assieme all'informazione.

5.4.2 Sicurezza della carta

I rischi di furto e falsificazione delle carte d'identità, con l'adozione del modello elettronico, sono notevolmente ridotti, principalmente in virtù della natura del supporto e delle garanzie di inalterabilità delle informazioni riportate, tanto sul chip che sulla banda ottica.

La banda ottica rappresenta l'elemento centrale della sicurezza per i motivi di seguito riportati.

La caratteristica di base della scrittura WORM (Write Once Read Many) non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili. Eventuali aggiornamenti consistono esclusivamente in aggiunte, proprio come avviene per un normale CD-Rom.

In ogni caso esistono le protezioni inserite nell'hardware di scrittura, in dotazione esclusivamente a E ed IPZS, e di ogni operazione effettuata dal funzionario autorizzato elettronicamente si tiene traccia presso SSCE.

Il controllo a vista della carta, inoltre, è garantito dalla presenza dell'Embedded Hologram che permette di effettuare un'azione di costante validazione dei dati stampati in chiaro e di evidenziarne immediatamente il tentativo di manomissione.

Infine non essendo la banda laser modificabile attraverso campi magnetici, calore (100°), campi elettrici, virus informatici, il suo contenuto è inattaccabile.

Gli eventuali interventi meccanici che modifichino strutturalmente o fisicamente la «card» sarebbero immediatamente visibili.

Relativamente al microchip, questi non permette - grazie alla sicurezza del suo stesso sistema operativo - di modificare o scrivere informazioni se non in presenza di determinate autorizzazioni.

Inoltre tutte le informazioni sensibili, tanto sul chip che sulla banda ottica, sono garantite contro l'alterazione, perché «firmate» digitalmente.

5.4.3 Furto della carta «attivata» o documento in bianco

La carta è in tale stato quando viene spedita da IPZS ai comuni, prima di essere formata e rilasciata.

In questo caso, dal momento che la personalizzazione richiede, per poter aver luogo, l'autenticazione del funzionario nei confronti del sistema e la firma dei dati da parte di appositi apparati contenenti la chiave privata dell'ente, tale eventualità rientra nella tipologia del «rilascio fraudolento» realizzabile solo attraverso l'infedeltà del funzionario stesso le cui attività però, con la citata tracciatura, restano registrate nel Data Base delle approvazioni presso SSCE.

5.4.4 Controlli a vista

L'intero circuito di sicurezza attraverso l'adozione dell'architettura a centralizzazione virtuale consente di innalzare il livello di qualità dei controlli, c.d. a vista, effettuati dalle Forze di Polizia per verificare l'identità delle persone sottoposte ai controlli stessi.

Disporre di un documento particolarmente attendibile consente di eseguire tutte le normali procedure in tempi molto ridotti con indubbio vantaggio per le persone coinvolte.

Le sicurezze adottate durante la fase di inizializzazione del documento, la presenza sulla banda ottica, sotto forma di ologramma, delle stesse informazioni grafiche, lo rendono molto più affidabile del modello cartaceo.

Laddove si volessero approfondire le verifiche, due sono le possibili soluzioni:

- Controllo dei dati autenticati e memorizzati nella banda ottica. Tramite apposito lettore opportunamente inizializzato, in grado di rilevare con certezza l'autenticità del documento
- Controllo delle informazioni presso il SSCE. Le Questure di competenza possono, collegandosi al SSCE, verificare immediatamente, grazie al possesso di opportune chiavi crittografiche, se le informazioni in esso contenute corrispondono con quelle riportate nel documento.

5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6, comma 2 del D.M.)

In attuazione dell'art. 6, comma 1, del D.P.C.M. 22 ottobre 1999, n. 437, presso il SSCE è presente un elenco dei documenti interdetti (black-list). Tale elenco è indispensabile per impedire l'operatività della CIE in caso di smarrimento o furto della stessa.

Le procedure da seguire per l'interdizione della carta vengono dettagliatamente descritte nei successivi paragrafi.

5.4.6 Software di sicurezza distribuito ai comuni (fa riferimento all'art. 6, comma 1 del D.M.)

Per procedere alla formazione ed all'emissione dei documenti, i Comuni devono collegarsi al SSCE. In assenza di tale collegamento qualsiasi documento prodotto verrebbe facilmente individuato come falso.

I requisiti per collegarsi al circuito di emissione sono un collegamento telematico, secondo i criteri stabiliti al paragrafo 3.2 del presente documento, e l'adozione di uno speciale software di sicurezza rilasciato dal Sistema di Sicurezza stesso.

Il SSCE curerà l'analisi, lo sviluppo, la distribuzione e la manutenzione del software, per motivi di riservatezza, di interoperabilità e di economicità.

Il software, unitamente alla chiave privata del comune, la prima volta dovrà essere ritirato presso il Ministero dell'Interno. Le release successive, invece, grazie alla disponibilità della chiave privata potranno essere prelevate direttamente via Web.

6. Servizi erogabili in rete (fa riferimento all'art. 5 del D.M.)

Le tipologie dei servizi erogabili possono, in sostanza, ricondursi a due: servizi standard che non necessitano di essere installati sul documento e servizi qualificati che richiedono l'installazione.

L'installazione di un servizio qualificato è il processo mediante il quale viene predisposta sulla carta la struttura dati del servizio, ovvero la chiave pubblica del server dell'ente erogatore od entrambi.

I livelli di sicurezza previsti per l'erogazione dei servizi sono:

- Autenticazione forte (strong authentication) del titolare
- Autenticazione forte del server erogatore (autenticazione esterna)
- Cifratura del canale (secure messaging)

Tali livelli di sicurezza possono essere contemporaneamente presenti; in particolare, il secure messaging implica sempre almeno l'autenticazione forte del server. Per tutti i tre livelli è necessaria la digitazione del PIN.

Nel caso dei servizi standard si accede al servizio con il semplice riconoscimento tramite digitazione del PIN e, laddove necessario, l'utilizzo del certificato della carta per la strong authentication.

Richiedono l'installazione sulla carta quei servizi che necessitano di informazioni aggiuntive da memorizzare sul documento. Per questi ultimi l'accesso al servizio avviene solo dopo che il Server che eroga il servizio ha riconosciuto, tramite un meccanismo basato su chiavi asimmetriche, la carta ed eventualmente dopo che quest'ultima ha riconosciuto il Server.

I servizi standard vengono erogati senza alcuna autorizzazione ed in piena autonomia dalle amministrazioni interessate ai titolari di carte e possono utilizzare solo il primo livello di autenticazione (autenticazione forte del titolare).

I servizi qualificati, se erogati da amministrazioni centrali, per poter essere installati devono essere previamente autorizzati. Tali servizi possono adottare tutti i livelli di sicurezza precedentemente elencati.

Rientra nei servizi qualificati la firma digitale disciplinata dal D.P.R. 513 del 1997. In questo solo caso, viene abilitata la funzione di generazione delle chiavi di sottoscrizione sottoponendola alle medesime condizioni di autenticazione del server remoto che gestisce l'operazione (possesso della chiave privata (Spri) corrispondente alla chiave pubblica (Spub) del server dell'ente certificatore).

6.1 Le liste dei servizi e la lista delle carte interdette (black-list)

Le liste dei servizi sono indispensabili per poter procedere all'installazione dei servizi qualificati sulla carta. Solo i servizi presenti in tale lista possono essere installati sulla carta.

Le liste dei servizi contengono almeno le seguenti informazioni:

- Identificativo del servizio
- Formato della struttura dati da creare sulla carta (se presente)
- Chiave di autenticazione del server erogatore (Spub)
- Spazio richiesto in EEPROM (memoria) del microcircuito
- Informazioni descrittive del servizio

Esistono due tipologie di liste dei servizi:

- La lista dei servizi nazionali (mantenuta da SSCE)
- Le liste dei servizi comunali (mantenute dai Comuni)

La lista nazionale presso il SSCE e le liste comunali interoperano secondo modalità e standard specifici. La lista nazionale contiene l'elenco dei servizi nazionali e l'elenco dei servizi ultracomunali.

Per servizi ultracomunali si intendono quelli che un Comune rende disponibili al di fuori della sua competenza territoriale.

Il software di sicurezza rilasciato ai comuni, al fine dell'installazione dei servizi, deve interoperare sia con la lista nazionale sia con l'eventuale lista comunale.

La predisposizione e la gestione della lista dei servizi comunali è affidata alla responsabilità del comune.

La predisposizione e la gestione della lista dei servizi nazionali è affidata al SSCE. Le amministrazioni centrali che intendono offrire servizi qualificati devono richiedere una autorizzazione al Dipartimento della Funzione Pubblica specificando i motivi per cui si ritiene necessario utilizzare questa tipologia di servizio, le modalità di installazione ovvero aggiornamento (nel caso si tratti di un servizio già esistente) e, in caso di parere favorevole, presentare al SSCE un documento in cui si evidenzia:

- la descrizione del servizio da erogare;
- le modalità tecniche attraverso le quali sarà garantito il servizio;
- l'organizzazione a supporto del sistema di erogazione del servizio.

Presso il SSCE è inoltre mantenuta la lista delle carte interdette (black-list), aggiornata secondo le modalità descritte al capitolo 8. Il SSCE mette a disposizione di tutti coloro che erogano servizi l'accesso telematico alla black-list. Saranno le caratteristiche del servizio che si deve erogare a stabilire la necessità di un accesso alla «black list» delle carte interdette.

6.2 Modalità di riconoscimento in rete

In considerazione dell'architettura definita per la carta d'identità elettronica e dell'utilizzo della componente microchip per il riconoscimento in rete della carta nei confronti di un server applicativo che eroga dei servizi, la soluzione che si è scelta è quella della Strong Authentication che richiede l'utilizzo di funzioni tipiche di una Public Key Infrastructure (SSCE).

6.2.1 Crypto Middleware ed API PKCS#11

Il Crypto Middleware è costituito dalle applicazioni (piattaforme) che SSCE mette a disposizione dei Client, che operano su reti aperte, per gestire i servizi di cifratura/decifratura.

Orientativamente, tali piattaforme svolgono le seguenti funzioni:

- Accesso LDAP ai servizi di Directory;
- Gestione in Cache della Certificate Revocation List;
- Parsing dei Certificati Digitali;
- Costruzione di strutture PKCS#7;
- Richiesta di certificazione di chiavi pubbliche;
- Richiesta di revoca di certificati
- Interfaccia ad alto livello verso le funzioni di cifratura.

Queste piattaforme, a loro volta, poggiano su strati software, o API, che le isolano dai dispositivi di cifratura, tipicamente le Smart Card.

Le API più comunemente usate sono le PKCS#11, le cui caratteristiche salienti sono:

- consentire ai Crypto Middleware di prescindere dai dispositivi che memorizzano chiavi e sviluppano crittografia;
- fornire ai Crypto Middleware una interfaccia standard;
- rendere portabili le applicazioni negli ambienti in cui la crittografia è trattata con queste API.

6.2.2 Processo di Strong Authentication

Questo processo consente la identificazione da remoto della carta per la fruizione dei servizi erogati da una applicazione residente presso una Pubblica Amministrazione Centrale.

Orientativamente, i passi previsti dalla procedura sono:

1. L'applicazione client stabilisce la comunicazione con l'applicazione server.
2. L'applicazione server richiede all'applicazione client il file «C_Carta» contenente il certificato (ID_Carta più la chiave pubblica Kpub della carta)
3. L'applicazione client interroga la carta e legge tale file mediante i comandi APDU SELECT FILE (C_Carta), READ BINARY.
4. L'applicazione client invia il file «C_Carta» al server.
5. L'applicazione server verifica la validità del certificato mediante SSCEpub ed estrae da esso ID_Carta e Kpub.
6. L'applicazione server genera una stringa di challenge e la invia al client rimanendo in attesa della risposta.
7. L'applicazione client seleziona Kpri mediante il comando MSE(Manage Security Environment). In tal modo Kpri è attivata e verrà usata in tutte le successive operazioni di cifratura effettuate dalla carta.

Mediante il comando PSO (Perform Security Operation) la carta esegue la cifratura del challenge usando Kpri precedentemente attivata, e restituisce all'applicazione client la stringa ottenuta. La chiave privata che è stata generata dalla carta in fase di inizializzazione, risulta invisibile dall'esterno e comunque impossibile estrarla dalla carta.

8. Il client invia al server in attesa il challenge firmato ricevuto dalla carta.

9. L'applicazione server verifica la stringa ricevuta e la confronta con il challenge precedentemente generato.

Se tale confronto ha esito positivo la carta è autenticata. A questo proposito è necessario che l'algoritmo di verifica, residente sul server, sia compatibile con quello usato dalla carta per cifrare il challenge.

6.2.3 Comandi di gestione utilizzati dalla Strong Authentication

La norma ISO 7816 parte 4 e parte 8 definisce, oltre alla struttura del File System, anche i comandi per interagire a livello applicativo. Tali comandi sono chiamati APDU (Application Protocol Data Unit).

In funzione dei passi procedurali del processo di Autenticazione sopra descritti, sono individuati i seguenti comandi APDU:

- SELECT FILE, per selezionare l'Elementary File che contiene il certificato della Carta di Identità Elettronica (C_Carta);
- READ BINARY, per leggere il certificato;
- MSE (Manage Security Environment), per attivare la chiave privata di autenticazione;
- PSO (Perform Security Operation), per cifrare il challenge da inviare alla applicazione server.

Un approccio che è stato scelto per garantire alle applicazioni di gestire in modo interoperabile la componente microchip della Carta di Identità Elettronica e quello di realizzare una libreria di interfaccia che implementi i comandi descritti precedentemente.

Tale libreria, realizzata da SSCE, metterà a disposizione presumibilmente le seguenti funzioni:- servizi di amministrazione;

- funzioni di interfaccia verso la CIE;
- identificazione Utente;
- selezione File;
- Read File;
- selezione chiave;
- autenticazione Interna;
- gestione errori ed anomalie.

6.3 Considerazioni sulla interoperabilità

Al momento della scrittura di questo documento, non esistono standard di riferimento che garantiscono l'interoperabilità dei sistemi di crittografia, per cui SSCE, per raggiungere questo obiettivo, ha ritenuto opportuno definire sia l'algoritmo crittografico di autenticazione, sia il formato del messaggio autenticato.

La scelta effettuata è quella di utilizzare RSA come algoritmo di autenticazione e PKCS#1 come formato; di seguito sono esposti i razionali che hanno condotto a questo tipo di soluzione.

6.3.1 Algoritmi

Gli algoritmi asimmetrici comunemente impiegati dalle Smart Card ed idonei per realizzare la autenticazione sono l'algoritmo RSA e l'algoritmo DSA.

Questi algoritmi sono onerosi dal punto di vista computazionale e quindi sono realizzati utilizzando un coprocessore aritmetico. La lunghezza della chiave dipende dalla capacità del coprocessore di effettuare moltiplicazioni in modulo. Questo comporta una lunghezza massima di chiave pari al massimo modulo supportato dal coprocessore per l'algoritmo

DSA ed una lunghezza massima pari al doppio del modulo per l'algoritmo RSA grazie alla possibilità di utilizzare il Chinese Remainder Theorem.

In virtù delle considerazioni precedenti la scelta effettuata è stata quella dell'algoritmo RSA in quanto consente di:

- poter scegliere tra una vasta gamma di fornitori;
- estendere, in futuro, la lunghezza della chiave.

6.3.2 Formati

I formati generalmente utilizzati dalla crittografia asimmetrica sono:

- il formato ISO 9796 parte 2;
- il formato PKCS#1.

Il formato ISO 9796-2 è adottato dallo standard EMV per l'autenticazione statica e dinamica.

In applicazioni non EMV questo formato è consigliabile quando l'intero processo di autenticazione comporta l'utilizzo di due Smart Card (Mutua autenticazione interna ed esterna).

Il formato PKCS#1 è consigliabile in quanto può essere considerato «standard de facto» ed i messaggi di autenticazione (Response) costruiti secondo questo formato possono essere verificati dalle applicazioni che utilizzano gli strumenti tipici delle Public Key Infrastructure.

6.4 Strong Authentication lato Server

Quanto affermato nei precedenti paragrafi è un solido punto di partenza per risolvere il problema della autenticazione forte in rete per quanto concerne il Client e la CIE. È ora necessario definire la componente server del processo di autenticazione.

6.4.1 Server Authentication Middleware

Il Server Authentication Middleware è lo strato software che fornisce i servizi crittografici alla Applicazione.

Le funzioni che questo strato rende disponibili sono:

- Generazione di quantità random;
- Funzioni di Hash;
- Gestione di Certificati digitali in formato X509v3;
- Verify Certificate (per validare il certificato della CIE)
- Verify Signature (per validare il messaggio di Autenticazione)
- Caricamento della Certificate Revocation List
- Gestione della Revocation List.

Quelle descritte sono solamente un subset delle funzionalità del Server Authentication Middleware in una Infrastruttura a Chiave Pubblica ma sono comunque sufficienti per considerare la possibilità di utilizzo di software di mercato.

I requisiti di questa componente software sono:

- servizi crittografici come descritto nei punti precedenti;
- interoperabilità con i Client;
- indipendenza degli strumenti di produzione dei certificati.

Il primo requisito è una funzionalità tipica dei Middleware crittografici, il secondo requisito è soddisfatto dalla scelta fatta per Algoritmo e Formato che rende univoca la struttura del messaggio di Autenticazione mentre il terzo requisito è garantito dal circuito di emissione della Carta di Identità Elettronica essendo la produzione dei certificati di competenza di SSCE.

6.5 Installazione dei servizi

L'installazione dei servizi avviene durante la fase di formazione e rilascio da parte dei comuni descritta in maniera analitica nel successivo capitolo 7.

6.6 Aggiornamento dei dati relativi alla fruizione dei servizi

Nei paragrafi precedenti è stato approfondito il tema della autenticazione della CIE verso un Ente in grado di erogare servizi, in questo paragrafo viene completato il processo di autenticazione specificando le procedure che permettono alla CIE di verificare l'autenticità del servizio remoto con cui sta interagendo. Questo processo è chiamato: Autenticazione Esterna

Un altro tema trattato in questo paragrafo è il caricamento remoto sicuro di dati nella CIE da parte dell'Ente che eroga il servizio, questo processo è chiamato Secure Messaging. I processi di Autenticazione e di Secure Messaging garantiscono l'interazione diretta tra Ente e Carta di Identità Elettronica e prevengono dai tentativi di intrusione che possono essere condotti sulla rete.

Il processo di autenticazione esterna utilizza metodologie di crittografia asimmetrica tramite la chiave pubblica del servizio (Spub) mentre il processo di secure messaging utilizza crittografia simmetrica.

Per quanto concerne la gestione delle chiavi simmetriche sono stati oggetto di valutazione i seguenti due metodi:

- quello basato sullo utilizzo di «diversified key» (Ks) derivate da «master key» (Km) e caricate nella CIE durante la fase di Installazione dei servizi;
- quello basato sullo scambio di una chiave di sessione (Ks) generata in modo casuale dalla CIE e crittografata ed autenticata dalla CIE stessa.

Il primo metodo è consolidato e comunemente impiegato nelle applicazioni Smart Card Based ma richiede particolare attenzione nella custodia e distribuzione delle chiavi.

Il secondo metodo, in fase di valutazione, richiede la scrittura di un comando ad hoc che consente la generazione, la crittografia e la autenticazione della chiave di sessione all'interno della CIE al fine di garantire alla Applicazione Server che quella chiave può essere decrittografata solo da lei e generata solamente dalla CIE.

6.7 Autenticazione esterna

Il processo di autenticazione esterna è attivato dall'applicazione remota che deve poter accedere ai file della Carta di Identità Elettronica per aggiornarne i dati.

Questo processo utilizza la chiave pubblica del servizio (Spub) che è stata caricata nella carta durante la fase di installazione del servizio.

L'Autenticazione Esterna coinvolge i seguenti moduli:

- applicazione Server
- applicazione Client
- libreria di interfaccia e CIE.

La Figura [5] schematizza un esempio di flusso di informazioni scambiate tra i vari moduli che concorrono al processo di autenticazione esterna.

Il processo di Autenticazione Esterna è attivato dalla applicazione Server dopo che è stata riconosciuta (autenticata) la Carta ed il titolare.

Orientativamente, il processo di Autenticazione si svolge secondo i seguenti passi procedurali:

1. L'Applicazione Server richiede alla Applicazione Client di essere autenticata dalla CIE (ad es. tramite il comando «Aut_Request»);
2. L'applicazione Client, servendosi della LIBRERIA, invia una «challenge» alla CIE (ad es. con il comando «Get_Challenge»);
3. La risposta della CIE è un numero random (il Challenge);
4. L'Applicazione Client invia alla Applicazione Server il numero random generato dalla CIE (ad es. con il comando «Aut_Challenge»);
5. L'Applicazione Server firma il Challenge con la chiave privata del servizio (Spri), e lo invia alla Applicazione Client (ad es. con il comando «Auth_Response»);
6. La applicazione Client, servendosi della libreria, richiede alla CIE un'operazione di «autenticazione esterna»;

7. La CIE utilizza la chiave pubblica del servizio (Spub), relativa alla directory a cui si vuole accedere, per verificare la autenticità del Response; se la verifica è positiva viene inviato un messaggio di consenso alla Applicazione Client tramite la libreria e viene reso disponibile l'accesso ai file appartenenti a quella directory;

8. L'Applicazione Client comunica alla Applicazione Server l'esito del processo (ad es. tramite il messaggio «Auth_Result»);

Nella descrizione del processo di Autenticazione Esterna si sono trascurati dettagli procedurali quali la gestione delle eventuali anomalie e le «Retry» tipiche di questi processi in quanto non incidono sulle funzionalità della CIE.

6.8 Secure Messaging

Il processo di Secure Messaging è attivato dopo i processi di autenticazione e consente lo scambio dati crittografato tra CIE ed Applicazione Server.

Esso utilizza una chiave di sessione diversificata KD che è:

- derivata da KS attraverso la generazione di una quantità Random, qualora venga scelto di distribuire le chiavi secondo metodi convenzionali durante la fase di emissione;
- coincidente con la chiave KS autogenerata in modalità casuale, qualora venga scelta la distribuzione delle chiavi di sessione dalla CIE alle Applicazioni Server con un apposito comando basato sull'utilizzo di crittografia asimmetrica.

Il comando di Secure Messaging dovrà essere implementato secondo la norma ISO 7816-4 nella modalità «Secure Messaging for Confidentiality».

7. Processo di Emissione

Nel presente capitolo sono descritte in dettaglio le fasi operative previste dal circuito d'emissione.

Per una migliore comprensione del processo d'emissione si riporta un glossario di riferimento.

7.1 Produzione di banda laser e microprocessore

I Fornitori di microprocessori (Fp) ed i Fornitori di bande ottiche (Fb) provvedono alla fabbricazione dei supporti informatici.

I Fornitori di microprocessori provvedono anche alla mascheratura in ROM del Sistema Operativo.

Entrambi i fornitori applicano, in fase di produzione, un numero seriale progressivo univoco, sui supporti informatici da loro forniti e predispongono una distinta, cartacea ed elettronica, che riporta le seguenti indicazioni: ID fornitore, numero seriale, numero del lotto di produzione, data di produzione.

I fornitori, successivamente inviano i loro prodotti, accompagnati dalle distinte, direttamente all'Istituto Poligrafico dello Stato (IPZS).

7.2 Produzione ed inizializzazione della carta d'identità elettronica e del documento elettronico

Per meglio comprendere le diverse fasi del circuito di emissione, è bene fare dei brevi cenni sull'organizzazione e sulla normalizzazione delle informazioni sui supporti informatici della CIE.

7.2.1 Struttura delle informazioni sulla banda ottica

Sulla banda ottica vi sono due aree di memorizzazione differenti ma sincrone:

- Una area dati che contiene, codificati in record di formato opportuno (Rd), i necessari dati della carta, del titolare e i servizi installati.- Una area di controllo che contiene, codificate in formato opportuno (Rc), le informazioni di controllo e verifica dei corrispondenti Rd.

L'area controllo è assimilabile ad un registro incrementale delle operazioni avvenute sulla carta, e consente di stabilire con certezza chi, dove e quando ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato dei «sigilli» apposti da:

- Istituto Poligrafico dello Stato;
- comuni;

- SSCE.

A ciascun record Rd dell'area dati corrisponde un record Rc dell'area di controllo. I record dati possono avere formati multipli secondo necessità.

I record Rd dell'area dati sono formati da IPZS e da E. I record Rc dell'area di controllo sono composti da due parti: una formata da IPZS e da E, l'altra formata da SSCE.

Questi record contengono dunque richieste (di IPZS o E) ed approvazioni (di SSCE), e permettono di far avanzare la carta da uno stato all'altro, lungo il «percorso» che la porta dalla manifattura fino al momento del rilascio al titolare.

Questo flusso di richiesta ed approvazione è lo stesso utilizzato anche per il microcircuito, per cui nel record di controllo sono presenti elementi che andranno poi memorizzati nel chip (come il certificato C_Carta), e che consentono in tal modo anche un utile corrispondenza dei dati tra chip e banda ottica.

La tabella seguente definisce la struttura (campi) del record di controllo:

La seguente tabella definisce la struttura (campi) del record dati.

7.2.2 Struttura delle informazioni nel microprocessore

La successiva tabella definisce la struttura dei dati registrati nella memoria riscrivibile (EEPROM) del microcircuito.

Fornito da: indica l'operazione in ragione della quale viene messo a disposizione un contenuto informativo, consistente in una sequenza di bytes. Ad esempio, il risultato della raccolta dei dati personali del titolare, effettuata dall'ente emettitore (il comune).

Predisposto da: indica l'operazione di creazione di una nuova struttura dati (DF o EF), ossia un «contenitore» vuoto, pronto ad essere riempito con le informazioni che risultano da un'operazione del tipo precedente.

Scritto da: è l'operazione con la quale un contenitore vuoto (EF) viene riempito con le informazioni che risultano da una precedente operazione di generazione.

7.3 Le fasi preliminari

L'Istituto Poligrafico, responsabile della manifattura della CIE, riceve dalle Prefetture, in via telematica, le richieste di fornitura di «documenti in bianco», distinte per Comune, e dai fornitori i microprocessori e le bande ottiche.

La consegna, alle Prefetture, dei «documenti in bianco» avviene al termine delle seguenti sottofasi di generazione numeri identificativi, produzione, inizializzazione ed incisione grafica degli elementi costanti.

7.3.1 Generazione numeri identificativi per le carte d'identità ed i documenti elettronici.

L'IPZS richiede al SSCE i numeri identificativi (ID-Carta) necessari;

SSCE genera i nuovi ID-Carta ed inserisce un equivalente numero di record «in attesa» di divenire CEE nel suo database centrale;

L'IPZS riceve via telematica i lotti di numeri identificativi da assegnare alle nuove carte in corso di produzione.

7.3.2 Produzione

L'IPZS, attiva le procedure necessarie ai fini della:

- predisposizione del supporto fisico;
- inserimento nel supporto fisico della pellicola di banda ottica e del microprocessore;
- stampa del logo e degli elementi grafici costanti e di sicurezza;
- inizializzazione elettrica del microprocessore.

7.3.3 Inizializzazione

La sottofase di inizializzazione, una delle più delicate dell'intero processo di emissione, consente di trasformare i tre supporti previsti, in un unico elemento inscindibile.

Dopo la fase di integrazione fisica del supporto plastico, con la banda ottica ed il microprocessore, l'inizializzazione provvede alla integrazione logica tramite l'apposizione di codici univoci.

Mentre risulta di immediata applicazione il codice apposto graficamente sul supporto fisico, l'inizializzazione di quelli informatici ha quale prerequisito la loro «formattazione» che, di fatto, consiste nella loro strutturazione in «directory» e l'impostazione delle condizioni di test necessarie a definire i diritti di accesso alle directory.

Le directory, definite in dettaglio nei precedenti paragrafi, servono per tracciare tutte le fasi di inizializzazione e personalizzazione della Carta, per consentire l'installazione dei servizi qualificati e per normalizzare i dati identificativi del titolare, le informazioni alfanumeriche nonché le immagini.

In particolare, IPZS provvede alla:

- generazione della struttura dati interna della banda ottica;
- generazione della struttura dati interna del microprocessore;
- scrittura dei files elementari che riportano i dati specifici del microprocessore («Dati-processore»), della banda ottica («Dati banda ottica») e del sistema operativo («Parametri-APDU»);
- scrittura ID-Carta;
- impostazione delle condizioni di accesso a tali file;
- scrittura del record dati (Rd) e di alcuni campi (1-6) di quello di controllo (Rc) relativi all'operazione di inizializzazione. Il record di controllo deve contenere almeno:
 - ID Carta;
 - Dati Processore/Dati Banda Ottica;
 - Data di fabbricazione;
 - PIN P1 (per abilitare l'accesso in scrittura dei files elementari che devono essere riempiti dal Comune al momento della formazione della carta) cifrato con la chiave pubblica del comune).
- Indicazione della Provincia e del comune cui la carta è destinata.
- inserimento del record dati e di quello di controllo in coda ad un file di richieste di autorizzazione da inviare a SSCE;
- stampa dello sfondo, del Logo, del numero di carta (ID Carta, quello generato da SSCE) e degli altri elementi costanti;
- incisione grafica sulla banda ottica (Embedded Hologram) degli elementi costanti e dell'ID-Carta;
- stoccaggio della carta.

7.3.4 Attivazione

Al termine della presente sottofase la carta d'identità risulta «attivata», e diventa «documento in bianco», ossia pronto alla fase successiva di formazione e rilascio, ad opera dei Comuni.

Durante la presente sottofase l'IPZS esegue le seguenti attività:

- riceve da SSCE il file di approvazione per attivare il lotto di carte in lavorazione;
- inserisce le carte, che fanno parte del lotto autorizzato, nello/negli apparati per la lettura del chip e della banda ottica e legge l'ID-Carta contenuto nei due supporti (la lettura in entrambi i supporti costituisce un ulteriore controllo sui dati inseriti);
- trasmette a SSCE le associazioni ID-Carta/Provincia richiedente;
- invia le carte in bianco attivate alle Prefetture. Queste ultime sono, a loro volta, incaricate della distribuzione nella provincia di loro competenza agli enti autorizzati alle procedure di emissione (Comuni E).

Al completamento di questa fase il data base di SSCE conterrà tanti record quante sono le carte in bianco in attesa di formazione. Tali record contengono già informazioni come il numero identificativo della carta (ID-Carta), la Provincia ed il Comune di destinazione.

Durante la fase di personalizzazione i campi di tali record verranno ulteriormente popolati con i codici fiscali (scritti in chiaro) dei titolari e con i dati identificativi (scritti in forma cifrata) degli stessi.

La cifratura avverrà, tramite un sistema automatico, utilizzando la chiave pubblica della Questura, territorialmente competente, e quella del comune che ha rilasciato la Carta d'Identità Elettronica.

7.4 Personalizzazione ed emissione delle carte

La formazione delle carte ed il loro rilascio è condotta direttamente dai Comuni. Nei paragrafi successivi le chiavi asimmetriche saranno indicate con la seguente notazione:

- Kpri-aut, chiave privata di autenticazione;
- Kpub-aut, chiave pubblica di autenticazione;
- Kpub-enc, chiave privata di crittografia;
- Kpub-enc, chiave pubblica di crittografia.

7.4.1 Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)

Il comune per il tramite delle Prefetture della propria provincia, riceve i documenti in bianco;

I documenti devono essere conservati dai comuni in appositi armadi di sicurezza, possibilmente in locali ad accesso riservato.

7.4.1.1 Sottofase di Compilazione

- Il Comune riceve i «documenti in bianco» da parte della Prefettura;
- tramite il software di sicurezza, le informazioni del titolare sono riportate dal comune nel sistema.

I dati sono quelli indicati in dettaglio al paragrafo 4.4.

La fotografia può essere catturata direttamente, tramite videocamera digitale o digitalizzata per mezzo di uno scanner.

Anche per digitalizzare la firma del titolare può essere utilizzato uno scanner oppure può essere catturata direttamente tramite tavoletta grafica.

Per l'impronta digitale, laddove il comune decida di assumerla o il richiedente desideri inserirla nella propria CiE, è necessario utilizzare un lettore di impronte digitali (live scan);

- Generazione della coppia di chiavi Kpub e Kpri (della carta) necessarie per garantire l'autenticazione in rete della carta e generazione del relativo PIN utente. La generazione di queste chiavi avviene all'interno del microprocessore.
- Cifratura simmetrica dei dati a 128 bit. La cifratura viene eseguita automaticamente dal software di sicurezza. La cifratura è indispensabile per proteggere i dati durante la trasmissione al SSCE utilizzando la Kpub-enc del SSCE stesso con una chiave di trasporto da 128 bit generata in maniera dinamica sessione per sessione;
- Apposizione del bollo elettronico del comune, per mezzo della Kpri-aut (Comune). L'apposizione di tale bollo garantisce il mittente al SSCE;
- Invio della richiesta di emissione carta d'identità al SSCE per via telematica.

7.4.1.2 Sottofase di autorizzazione

La sottofase di autorizzazione viene effettuata dal SSCE quando, da un qualsiasi comune, riceve una richiesta di rilascio di una nuova CIE. Vengono eseguite le seguenti attività:

- 1) SSCE riceve i dati raccolti dal comune;
- 2) SSCE estrae, tramite la propria Kpri-enc, il record dati;
- 3) SSCE mantiene in chiaro codice fiscale, provincia e comune richiedente e cifra tutte le altre informazioni con due chiavi: la Kpub-aut, del comune richiedente e la Kpub-aut della Questura territorialmente competente;
- 4) SSCE esegue il controllo automatico di «non esistenza» sulla propria base dati, tramite i dati in chiaro e la Kpub della CIE;
 - a) Controllo positivo (es. CIE già rilasciata per quel codice fiscale, richiesta avanzata da un comune diverso da quello previsto e soprattutto che la Kpub della CIE non sia identica ad una già certificata, etc.) viene rigettata la richiesta non vengono seguite ulteriori attività e all'ente emettitore viene ritornato un opportuno codice di errore.
 - b) Controllo negativo (la richiesta può essere soddisfatta).

5) SSCE trasmette l'esito dell'operazione di autorizzazione. I dati vengono inviati cifrati utilizzando la Kpub-enc del Comune ed una chiave di trasporto a 128 bit generata sessione per sessione e certificati con il bollo elettronico del SSCE (Kpri-aut di SSCE).

7.4.1.3 Sottofase di formazione

Sottofase di competenza dell'Ente emittitore che riporta i dati su tutti i supporti: microprocessore, banda ottica e grafici sul supporto fisico. La criticità maggiore sta nel fatto che, qualsiasi inconveniente possa verificarsi non deve mettere a rischio l'integrità dei dati (per es. scrivendo informazioni diverse sui vari supporti). Allo scopo si suggerisce di garantire agli strumenti informatici continuità elettrica.

1) E riceve il record dati validato da SSCE;

2) memorizza i dati nel microprocessore;

3) memorizza i dati nella banda ottica. Al fine di garantire l'allineamento delle informazioni il lettore/scrittore di banda ottica dovrebbe avere la possibilità di leggere anche il microprocessore. Al fine di consentire una identificazione sicura, e dare certezza sulla originalità della CIE, i dati memorizzati nella banda ottica devono essere quelli firmati con il bollo elettronico del SSCE.

4) stampa grafica dei dati sul supporto fisico. Anche in questo caso sarebbe opportuno che la stampante sia in grado di leggere il microprocessore.

5) stampa del PIN utente su speciale carta chimica retinata, tale da garantire la riservatezza dell'informazione contenuta e di evidenziare eventuali tentativi di apertura.

7.4.1.4 Sottofase di rilascio

Anche questa sottofase è di esclusiva competenza dei comuni che:

1) rilasciano la CIE al cittadino che ne ha fatto richiesta;

2) consegnano la busta conte.

3) comunicano a SSCE l'avvenuto rilascio tramite comunicazione telematica diretta.

7.4.1.5 Sottofase di verifica e controllo

La verifica ed il controllo sono le uniche attività sempre presenti in tutte le sottofasi di lavorazione della CIE, dal momento della produzione fino al loro rilascio e vengono condotte da SSCE. Per questo motivo tutti gli enti coinvolti nei vari momenti del processo devono disporre di una connessione telematica con il Sistema.

Ovviamente la verifica ed il controllo citato nel processo di formazione, non è riferito a quello che verrà dettagliato nel capitolo successivo che, invece, si riferisce ai controlli effettuabili dalla Polizia come previsto dal Testo Unico delle Leggi di P.S.

8. Verifica delle carte di identità elettroniche (fa riferimento all'art. 6, comma 1 del D.M.)

Nel presente capitolo sono descritti in dettaglio i casi in cui è consentito l'accesso alle CIE ed alle informazioni in esse contenute. Vengono, altresì, indicati gli organi competenti e le modalità di accesso.

8.1 Conservazione del cartellino elettronico (fa riferimento all'art. 6, comma 3 del D.M.)

Il processo di ammodernamento della CIE deve necessariamente portare ad una differente interpretazione di alcune delle norme precedenti, soprattutto di quelle destinate alla gestione del modello cartaceo, ormai superato.

È pressoché intuitivo come non trovino ragione di essere le prescrizioni relative alla conservazione e consultazione della copia del cartellino presente in ciascuna Questura. L'obbligo previsto per i Comuni di trasmettere copia del cartellino per ogni carta di identità rilasciata, viene sostituito dalla seguente procedura prevista per il nuovo cartellino elettronico:

- i Comuni eseguono le attività di formazione e rilascio delle CIE;

- SSCE riceve comunicazione che è stata rilasciata la CIE e memorizza la copia elettronica, della stessa, nell'archivio della Questura territorialmente competente. La copia elettronica, viene cifrata con la chiave pubblica della Questura stessa. Tale modalità

consente di attendere al Testo Unico delle Leggi di P.S. che indica nelle Questura l'ufficio a cui è demandata la conservazione della copia delle CIE;

- i controlli sulle CEE, una volta memorizzate, possono essere effettuati secondo le seguenti modalità:

- da qualsiasi operatore delle Forze di Polizia tramite controlli a vista, apparecchiature stand-alone (lettori di banda ottica) o transazioni a SSCE. In quest'ultimo caso, se la richiesta arriva da una Questura di una Provincia diversa da quella dove è stata rilasciata la CIE, l'operatore può, tramite il codice fiscale del titolare o il numero della CEE verificarne l'esistenza, il comune e la provincia in cui è stata rilasciata, non può vedere nel dettaglio le informazioni della CIE;

- da un operatore della Questura nella cui Provincia è stata rilasciata la CIE. In questo caso l'operatore può, tramite il codice fiscale del titolare o il numero di CIE, verificarne l'esistenza e, tramite l'inserimento della propria chiave privata, verificarne anche il contenuto nel dettaglio.

- le Questure territorialmente competenti tramite SSCE conservano e consultano la copia elettronica della CIE. Possono eseguire anche stampe e tutte le attività già possibili con la passata gestione.

8.2 Interdizione dell'operatività della CEE (fa riferimento all'art. 6, comma 2 del D.M.)

Le caratteristiche principali della nuova CIE, che la differenziano dal vecchio modello cartaceo, sono rappresentate dalla presenza dei supporti informatici e dalla gestione centralizzata del flusso di emissione. Entrambi gli elementi da un lato aumentano il livello di sicurezza del nuovo documento e dall'altro offrono la possibilità di accesso a servizi telematici sia nazionali che locali.

Proprio questa nuova possibilità di accedere a servizi implica la necessità di dover interdire, più che in passato, l'utilizzo della CIE che potrebbe essere impiegata, in caso di furto o smarrimento, da persone diverse dal titolare.

Nel seguito vengono descritte le modalità a cui è necessario attenersi in caso di furto o smarrimento di una CIE.

- il titolare telefona al numero verde e comunica l'avvenuto smarrimento/furto della CIE;

- per motivi di sicurezza, l'interdizione temporanea della CIE avviene dopo che è stata svolta una successiva verifica telefonica;

- a seguito di tale comunicazione nel record relativo alla CIE viene apposto un «flag» e, per un periodo di 7 (sette) gg, la CIE non è in grado di accedere a servizi;

- successivamente alla comunicazione telefonica, il titolare della CIE deve presentare regolare denuncia ad un ufficio di Polizia;

- la denuncia viene trasmessa alla Questura della Provincia dove è stata rilasciata la CIE;

- la Questura inibisce, definitivamente, l'utilizzo in rete della CIE ed il titolare può richiedere un duplicato, recandosi al comune;

- se durante i sette gg. di interdizione momentanea non viene applicata l'interdizione definitiva, la CIE torna ad essere, nuovamente, «NON interdetta».

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 31 ottobre 2000

Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'art. 15 comma 2, della legge 15 marzo 1997, n. 59, e successive modificazioni ed integrazioni;

Visto l'art. 17, comma 19, della legge 15 maggio 1997, n. 127, e successive modificazioni ed integrazioni;

Visti gli articoli 4, 6 e 17 del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428;

Visto il decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni;

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

Visto l'art. 1, lettera h), del decreto del Presidente del Consiglio dei Ministri dell'8 maggio 2000, recante delega di funzioni in materia di innovazione tecnologica e dei sistemi informatici e telefonici al Ministro per la funzione pubblica sen. prof. Franco Bassanini;

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

Decreta:

Titolo I

Ambito di applicazione, definizioni ed obiettivi di adeguamento delle pubbliche amministrazioni

Art. 1. Ambito di applicazione

1. Il presente decreto stabilisce le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione di protocollo, di cui all'art. 4, comma 4, del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428, nonché il formato e la struttura delle informazioni associate al documento informatico, di cui all'art. 6, comma 5, del medesimo decreto.

2. Il presente decreto stabilisce altresì le regole tecniche, i criteri e le specifiche delle informazioni previste, delle operazioni di registrazione e del formato dei dati relativi ai sistemi informatici per la gestione dei flussi documentali, di cui all'art.

17, comma 1, del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.

Art. 2. Definizioni

1. Ai fini del presente decreto si intendono per:

a) "decreto del Presidente della Repubblica n. 428/1998", il decreto del Presidente della Repubblica 20 ottobre 1998, n. 428;

b) "decreto n. 29/1993", il decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni;

c) "legge n. 127/1997", la legge 15 maggio 1997, n. 127, e successive modificazioni ed integrazioni;

d) "decreto del Presidente della Repubblica n. 513/1997", il decreto del Presidente della Repubblica 10 novembre 1997, n. 513;

- e) "delibera AIPA 24/98", la deliberazione 30 luglio 1998, n. 24, dell'Autorita' per l'informatica nella pubblica amministrazione recante regole tecniche per l'uso di supporti ottici;
- f) "funzionalita' minima", la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'art. 7 del decreto del Presidente della Repubblica n. 428/1998;
- g) "funzionalita' aggiuntive", le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonche' alla accessibilita' delle informazioni;
- h) "sistema di classificazione", lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attivita' dell'amministrazione interessata;
- i) "funzionalita' interoperative", le componenti del sistema finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'art. 11 del decreto del Presidente della Repubblica n. 428/1998;
- l) "sessione di registrazione", ogni attivita' di assegnazione delle informazioni nella operazione di registrazione di protocollo effettuata secondo le modalita' previste dall'art. 4, comma 3, del decreto del Presidente della Repubblica n. 428/1998;
- m) "responsabile del servizio", il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'art. 12 del decreto del Presidente della Repubblica n. 428/1998;
- n) "area organizzativa omogenea", un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'art. 2, comma 2, del decreto del Presidente della Repubblica n. 428/1998;
- o) "ufficio utente" di una area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.

Art. 3. Obiettivi di adeguamento delle pubbliche amministrazioni

1. Le pubbliche amministrazioni di cui al decreto n. 29/1993 perseguono, ciascuna nell'ambito del proprio ordinamento, nel tempo tecnico necessario, e comunque entro i termini indicati dall'art. 21 del decreto del Presidente della Repubblica n. 428/1998, i seguenti obiettivi di adeguamento organizzativo e funzionale:

- a) l'individuazione delle aree organizzative omogenee e dei relativi uffici di riferimento ai sensi dell'art. 2 del decreto del Presidente della Repubblica n. 428/1998;
- b) la nomina del responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 12 del decreto del Presidente della Repubblica n. 428/1998, e conseguentemente la nomina di un suo vicario, per casi di vacanza, assenza o impedimento del primo su proposta del medesimo;
- c) l'adozione, dopo la nomina del responsabile del servizio e sulla sua proposta, del manuale di gestione di cui all'art. 5 del presente decreto;
- d) la definizione, su indicazione del responsabile del servizio, dei tempi, delle modalita' e delle misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, piu' in generale, dei protocolli diversi dal protocollo informatico previsto dal decreto del Presidente della Repubblica n. 428/1998.

Art. 4. Obiettivi e compiti particolari del responsabile del servizio

1. In attuazione dell'art. 12 del decreto del Presidente della Repubblica n. 428/1998, le pubbliche amministrazioni di cui al decreto n. 29/1993 provvedono a definire le attribuzioni del responsabile del servizio in modo da assicurargli, in particolare, il compito di:

- a) predisporre lo schema del manuale di gestione di cui all'art. 5 del presente decreto, che deve essere adottato dalle pubbliche amministrazioni di cui al decreto n. 29/1993 ai sensi dell'art. 2, comma 1, lettera c), del presente decreto;
- b) proporre i tempi, le modalita' e le misure organizzative e tecniche di cui all'art. 3, comma 1, lettera d), del presente decreto;
- c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il responsabile dei sistemi informativi automatizzati e con il responsabile della sicurezza dei dati personali di cui alla legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, e nel rispetto delle misure minime di sicurezza previste dal regolamento di attuazione emanato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318, in attuazione dell'art. 15, comma 2, della citata legge n. 675/1996.

Art. 5.

Manuale di gestione

1. Il manuale di gestione descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio.

2. Nel manuale di gestione sono riportati, in particolare:

- a) la pianificazione, le modalita' e le misure di cui all'art. 3, comma 1, lettera d), del presente decreto;
- b) il piano di sicurezza dei documenti informatici di cui all'art. 4, comma 4, del presente decreto;
- c) le modalita' di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'area organizzativa omogenea;
- d) la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalita' di trasmissione, tra i quali, in particolare, documenti informatici di fatto pervenuti per canali diversi da quelli previsti dall'art. 15 del presente decreto, nonche' fax, raccomandata, assicurata;
- e) l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione e/o verso altre amministrazioni;
- f) l'indicazione delle unita' organizzative responsabili delle attivita' di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea;
- g) l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 4, comma 5, del decreto del Presidente della Repubblica n. 428/1998;
- h) l'elenco dei documenti soggetti a registrazione particolare e le relative modalita' di trattamento;

i) il sistema di classificazione, con l'indicazione delle modalita' di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, anche con riferimento all'uso di supporti sostitutivi;

l) le modalita' di produzione e di conservazione delle registrazioni di protocollo informatico ed in particolare l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire la non modificabilita' della registrazione di protocollo, la contemporaneita' della stessa con l'operazione di segnatura ai sensi dell'art. 6 del decreto del Presidente della Repubblica n. 428/1998, nonche' le modalita' di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attivita' di registrazione;

m) la descrizione funzionale ed operativa del sistema di protocollo informatico con particolare riferimento alle modalita' di utilizzo;

n) i criteri e le modalita' per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;

o) le modalita' di utilizzo del registro di emergenza ai sensi dell'art. 14 del decreto del Presidente della Repubblica n. 428/1998, inclusa la funzione di recupero dei dati protocollati manualmente.

3. Il manuale di gestione e' reso pubblico dalle pubbliche amministrazioni di cui al decreto n. 29/1993 secondo le modalita' previste dai singoli ordinamenti. Esso puo' altresì essere reso accessibile al pubblico per via telematica ovvero su supporto informatico o cartaceo.

Titolo II

Il sistema di protocollo informatico

Art. 6. Funzionalita'

1. Il sistema di protocollo informatico comprende almeno la "funzionalita' minima".
2. Le pubbliche amministrazioni di cui al decreto n. 29/1993 valutano l'opportunita' di acquisire o realizzare le funzionalita' aggiuntive sulla base del rapporto tra costi e benefici nell'ambito dei propri obiettivi di miglioramento dei servizi e di efficienza operativa.
3. Le funzionalita' aggiuntive condividono con la funzionalita' minima almeno i dati identificativi dei documenti.

Art. 7. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

1. Il sistema operativo dell'elaboratore, su cui viene realizzato il sistema di protocollo informatico, deve assicurare:
 - a) l'univoca identificazione ed autenticazione degli utenti;
 - b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
 - c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
 - d) la registrazione delle attivita' rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne la identificazione.
2. Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
3. Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.
4. Le registrazioni di cui ai commi 1, lettera d), e 3 del presente articolo devono essere protette da modifiche non autorizzate.
5. Al fine di garantire la non modificabilita' delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, deve essere

riversato su supporti informatici non riscrivibili e deve essere conservato da soggetto diverso dal responsabile del servizio appositamente nominato da ciascuna amministrazione.

6. L'autorità per l'informatica nella pubblica amministrazione compila e mantiene aggiornata la lista dei sistemi operativi disponibili commercialmente che soddisfano i requisiti minimi di sicurezza e la rende pubblica sul proprio sito internet.

Art. 8. Annullamento delle informazioni registrate in forma non modificabile

1. Fra le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile l'annullamento anche di una sola di esse determina l'automatico e contestuale annullamento della intera registrazione di protocollo.

2. Delle altre informazioni, registrate in forma non modificabile, l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica; così analogamente per lo stesso campo, od ogni altro, che dovesse poi risultare errato.

3. Le informazioni originarie, successivamente annullate, vengono memorizzate secondo le modalità specificate nell'art. 5, comma 1, del decreto del Presidente della Repubblica n. 428/1998.

Art. 9. Formato della segnatura di protocollo

1. Le informazioni apposte o associate al documento mediante l'operazione di segnatura di cui all'art. 6, comma 1, del decreto del Presidente della Repubblica n. 428/1998 sono espresse nel seguente formato:

a) codice identificativo dell'amministrazione;

b) codice identificativo dell'area organizzativa omogenea;

c) data di protocollo secondo il formato individuato in base alle previsioni di cui all'art. 18, secondo comma, del presente decreto;

d) progressivo di protocollo secondo il formato specificato all'art. 8 del decreto del Presidente della Repubblica n. 428/1998.

Titolo III

Formato e modalità di trasmissione dei documenti informatici tra pubbliche amministrazioni

Art. 10. Principi generali

1. Le amministrazioni pubbliche di cui al decreto n. 29/1993, ai fini della trasmissione di documenti informatici soggetti alla registrazione di protocollo e destinati ad altra amministrazione, adottano i formati e le modalità definiti nel presente titolo.

2. Le amministrazioni pubbliche di cui all'art. 1, primo comma, del decreto legislativo n. 29/1993, realizzano nei propri sistemi di protocollo informatico, oltre alla "funzionalità minima", anche funzionalità interoperative che rispondono almeno ai requisiti di accesso di cui all'art. 11 del decreto del Presidente della Repubblica n. 428/1998.

Art. 11. Indice delle amministrazioni pubbliche e delle aree organizzative omogenee

1. Per facilitare la trasmissione dei documenti informatici tra le amministrazioni è istituito l'indice delle amministrazioni pubbliche e delle aree organizzative omogenee.

2. L'indice e' destinato alla conservazione e alla pubblicazione dei dati di cui all'art. 12, comma 1, del presente decreto relativi alle pubbliche amministrazioni di cui al decreto n. 29/1993 ed alle loro aree organizzative omogenee.

3. L'indice delle amministrazioni di cui al comma 2 e' gestito da un sistema informatico accessibile tramite un sito internet in grado di permettere la consultazione delle informazioni in esso contenute da parte delle amministrazioni e di tutti i soggetti pubblici o privati anche secondo una modalita' compatibile con il protocollo LDAP definito nella specifica pubblica RFC 1777 e successive modificazioni o integrazioni.

4. Il sistema informatico di cui al comma 3 assicura altresì la conservazione dei dati storici relativi alle variazioni intercorse nell'indice delle amministrazioni e delle rispettive aree organizzative omogenee, onde consentire il corretto reperimento delle informazioni associate ad un documento protocollato anche a seguito delle variazioni intercorse nella struttura delle aree organizzative omogenee dell'amministrazione mittente o destinataria del documento.

Art. 12. Informazioni sulle amministrazioni e le aree organizzative omogenee

1. Ciascuna pubblica amministrazione di cui al decreto n. 29/1993 che intenda trasmettere documenti informatici soggetti alla registrazione di protocollo deve accreditarsi presso l'indice di cui all'art. 11 del presente decreto fornendo almeno le seguenti informazioni identificative relative all'amministrazione stessa:

- a) denominazione dell'amministrazione;
- b) codice identificativo proposto per l'amministrazione;
- c) indirizzo della sede principale dell'amministrazione;
- d) elenco delle proprie aree organizzative omogenee.

2. L'elenco di cui al comma 1, lettera d), comprende, per ciascuna area organizzativa omogenea:

- a) la denominazione;
- b) il codice identificativo;
- c) la casella di posta elettronica dell'area prevista dall'art. 15, comma 3, del presente decreto;
- d) il nominativo del responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi;
- e) la data di istituzione;
- f) la eventuale data di soppressione;
- g) l'elenco degli uffici utenti dell'area organizzativa omogenea.

3. Il codice associato a ciascuna area organizzativa omogenea e' generato ed attribuito autonomamente dalla relativa amministrazione.

Art. 13. Codice identificativo dell'amministrazione

1. Il codice identificativo dell'amministrazione viene attribuito a seguito della richiesta di accreditamento dell'amministrazione nell'indice delle amministrazioni pubbliche e delle aree organizzative omogenee di cui all'art. 11 del presente decreto.

2. Il codice identificativo dell'amministrazione coincide con il codice identificativo proposto di cui all'art. 12, comma 1, lettera b), qualora esso risulti univoco.

Art. 14. Modalita' di aggiornamento dell'indice delle amministrazioni

1. Ciascuna amministrazione comunica tempestivamente all'indice ogni successiva modifica delle informazioni di cui all'art. 12, del presente decreto e la data di entrata in vigore delle modifiche.

2. Con la stessa tempestività ciascuna amministrazione comunica la soppressione ovvero la creazione di una area organizzativa omogenea specificando tutti i dati previsti dall'art. 12, comma 2, del presente decreto.

3. Le amministrazioni possono comunicare ciascuna variazione nell'insieme delle proprie aree organizzative omogenee di cui ai commi 1 e 2 anche utilizzando i servizi telematici offerti dal sistema informatico di gestione dell'indice delle amministrazioni pubbliche.

Art. 15. Modalità di trasmissione e registrazione dei documenti informatici

1. Lo scambio dei documenti soggetti alla registrazione di protocollo e' effettuato mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

2. Ad ogni messaggio di posta elettronica ricevuto da una area organizzativa omogenea corrisponde una unica operazione di registrazione di protocollo. Detta registrazione si puo' riferire sia al corpo del messaggio sia uno o piu' file ad esso allegati.

3. Ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti.

L'indirizzo di tale casella e' riportato nell'indice delle amministrazioni pubbliche.

4. I messaggi di posta elettronica ricevuti da una amministrazione che sono soggetti alla registrazione di protocollo, vengono indirizzati, preferibilmente, alla casella di posta elettronica della area organizzativa omogenea destinataria del messaggio.

5. L'eventuale indicazione dell'ufficio utente, ovvero del soggetto, destinatario del documento, va riportata nella segnatura di protocollo secondo le modalità ed i formati previsti agli articoli 18 e 19 del presente decreto.

6. Ciascuna amministrazione stabilisce autonomamente le modalità di inoltro ed assegnazione dei documenti al singolo ufficio utente e le descrive nel manuale di gestione.

7. Qualora un documento informatico pervenga ad un ufficio utente di una area organizzativa omogenea per canali diversi da quello previsto al comma 1, e' responsabilità dell'ufficio stabilire, secondo quanto previsto dal manuale di gestione di cui al precedente art. 5, comma 2, lettera d), se il documento sia soggetto alla registrazione di protocollo ovvero a registrazione particolare di cui all'art. 4, comma 5, del decreto del Presidente della Repubblica n.

428/1998.

8. In aggiunta alle modalità di cui al presente titolo le amministrazioni possono utilizzare altre modalità di trasmissione di documenti informatici purché descritte nel manuale di gestione.

Art. 16. Leggibilità dei documenti

1. Ciascuna amministrazione garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti all'art. 6, comma 1, lettera b), della delibera AIPA n. 24/98 ovvero altri formati non proprietari.

Art. 17. Impronta del documento informatico

1. Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici l'impronta di cui all'art. 4, comma 1, lettera f), del decreto del Presidente della Repubblica n. 428/1998 va calcolata per tutti i file inclusi nel messaggio di posta elettronica.

2. La generazione dell'impronta si effettua impiegando la funzione di hash, definita nella norma ISO/IEC 10118-3:1998, Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

Art. 18. Segnatura di protocollo dei documenti trasmessi

1. I dati relativi alla segnatura di protocollo di un documento trasmesso da una area organizzativa omogenea sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML) 1.0 (raccomandazione W3C 10 febbraio 1998), compatibile con un file DTD (Document Type Definition) reso disponibile attraverso il sito internet di cui all'art. 11, comma 3, del presente decreto. Il file contiene le informazioni minime di cui al comma 1 del successivo art. 19. Le ulteriori informazioni definite al comma 2 del predetto articolo sono incluse nello stesso file.

2. L'Autorita' per l'informatica definisce ed aggiorna periodicamente con apposita circolare gli standard, le modalita' di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni associate ai documenti protocollati; ne cura la pubblicazione attraverso il proprio sito internet.

3. Per l'utilizzo di strumenti di firma digitale o di tecnologie riferibili alla realizzazione e gestione di una PKI, si applicano le regole di interoperabilita' definite con la circolare AIPA/CR/24 del 19 giugno 2000.

Art. 19. Informazioni da includere nella segnatura

1. Oltre alle informazioni specificate all'art. 9 le informazioni minime previste comprendono:

- a) l'oggetto;
- b) il mittente;
- c) il destinatario o i destinatari.

2. Nella segnatura di un documento protocollato in uscita da una amministrazione possono essere specificate opzionalmente una o piu' delle seguenti informazioni:

- a) indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verra' affidato il trattamento del documento;
- b) indice di classificazione;
- c) identificazione degli allegati;
- d) informazioni sul procedimento e sul trattamento.

3. Qualora due o piu' amministrazioni stabiliscano di scambiarsi informazioni non previste tra quelle definite al comma precedente, le stesse possono estendere il file di cui al comma 1 dell'art. 18, nel rispetto delle indicazioni tecniche stabilite dall'Autorita' per l'informatica, includendo le informazioni specifiche stabilite di comune accordo.

Art. 20. Realizzazione dell'indice delle amministrazioni

1. La realizzazione ed il funzionamento dell'indice di cui all'art.12 del presente decreto sono affidati al centro tecnico di cui all'art. 17, comma 19, della legge n. 127/1997.

Art. 21. Adeguamento delle regole tecniche

1. Le regole tecniche sono adeguate con cadenza almeno biennale a decorrere dalla data di entrata in vigore del presente decreto per assicurarne la corrispondenza con le esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche.

Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 ottobre 2000

p. Il Presidente: Bassanini

ADUNANZA DEL 23 NOVEMBRE 2000

DELIBERAZIONE N. 51/2000

Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

L'AUTORITÀ

Vista la legge 24 ottobre 1977, n. 801;

Vista la legge 7 agosto 1990, n. 241;

Visto il decreto legislativo 3 febbraio 1993, n. 29 e successive modificazioni ed integrazioni;

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

Visto l'articolo 2, comma 15, della legge 24 dicembre 1993, n. 537;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni;

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

Visto l'articolo 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;

Visto il decreto del Presidente della Repubblica 20 ottobre 1998, n. 428;

Visto il decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999;

Visto il decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto il decreto legislativo 29 ottobre 1999, n. 490;

D'intesa con l'Amministrazione degli Archivi di Stato;

DELIBERA

di emanare le seguenti regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513:

REGOLE TECNICHE IN MATERIA DI FORMAZIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI DELLE PUBBLICHE AMMINISTRAZIONI

Art. 1

Ambito di applicazione

1. La presente deliberazione detta norme in materia di documenti informatici non classificati formati e conservati dalle Pubbliche Amministrazioni.
2. Le regole tecniche di cui al comma 1 sono adeguate periodicamente dall'Autorità per l'informatica nella pubblica amministrazione alle esigenze istituzionali, organizzative, scientifiche e tecnologiche.

Art. 2

Definizioni

1. Ai fini della presente deliberazione s'intende:

- a) per amministrazioni pubbliche, tutte le Amministrazioni previste dall'art. 1, comma 2, del decreto legislativo 3 febbraio 1993, n. 29;

- b) per documento informatico, la rappresentazione informatica di atti, fatti e dati formati dalle amministrazioni pubbliche o, comunque, utilizzati ai fini dell'attività istituzionale ed amministrativa;
- c) per formazione, il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa;
- d) per conservazione, l'ordinata custodia di documenti informatici in modo da assicurarne l'integrità, l'affidabilità e la consultabilità nel tempo, anche attraverso idonei strumenti di ricerca;
- e) per formato, la modalità di rappresentazione del contenuto di un documento informatico;
- f) per sicurezza, l'insieme delle misure organizzative e tecniche finalizzate ad assicurare, senza soluzione di continuità, l'integrità, la disponibilità e la riservatezza dei documenti e degli archivi informatici;
- g) per accesso, la consultazione autorizzata, anche per via telematica, degli archivi e dei documenti informatici, sia per la tutela di situazioni giuridicamente rilevanti da parte di chi ne abbia interesse, sia per le attività amministrative;
- h) per archivio, l'insieme, organizzato e gestito in modo unitario per aree omogenee, costituito da uno o più supporti di memorizzazione, univocamente identificati, contenenti i documenti registrati.

Art. 3

Requisiti dei documenti informatici

1. La formazione e la conservazione dei documenti informatici delle pubbliche amministrazioni devono essere effettuate secondo i seguenti requisiti:
 - a) identificabilità del soggetto che ha formato il documento informatico e dell'amministrazione di riferimento;
 - b) sottoscrizione, quando prescritta, dei documenti informatici tramite la firma digitale ai sensi del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;
 - c) idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico, ai sensi del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428;
 - d) accessibilità ai documenti informatici tramite sistemi informativi automatizzati;
 - e) leggibilità dei documenti;
 - f) interscambiabilità dei documenti.
2. I documenti informatici, muniti dei requisiti sopra detti, sono validi e rilevanti a tutti gli effetti di legge.
3. Nella formazione e conservazione dei documenti informatici le pubbliche amministrazioni applicano le norme in materia di semplificazione e razionalizzazione delle attività amministrative e dei procedimenti.
4. Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dalla dirigenza, ai sensi dell'art. 3, comma 2, del decreto legislativo 3 febbraio 1993, n. 29, e con riferimento all'ordinamento delle rispettive amministrazioni.

Art. 4

Formato dei documenti informatici

1. I formati adottati devono possedere almeno i seguenti requisiti:
 - a) consentire, nei diversi ambiti di applicazione e per le diverse tipologie di trattazione, l'archiviazione, la leggibilità, l'interoperabilità e l'interscambio dei documenti;
 - b) la non alterabilità del documento durante le fasi di accesso e conservazione;
 - c) la possibilità di effettuare operazioni di ricerca tramite indici di classificazione o di archiviazione, nonché sui contenuti dei documenti;
 - d) l'immutabilità nel tempo del contenuto e della sua struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto;
 - e) la possibilità di integrare il documento informatico con immagini, suoni e video, purché incorporati in modo irreversibile e nel rispetto dei requisiti di cui alle lettere b) e d).

Art. 5

Sottoscrizione di documenti informatici

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
 - a) possono svolgere direttamente l'attività di certificazione ai sensi dell'art. 8 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513 solo per i propri organi ed uffici. In questo caso hanno l'obbligo di iscriversi nell'elenco pubblico dei certificatori presso l'Autorità per l'informatica nella pubblica amministrazione e devono attenersi alle regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999;
 - b) possono emettere certificati di firma digitale solo per i propri organi ed uffici ai sensi dell'art. 8 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, utilizzando i servizi offerti dal Centro tecnico o dai certificatori iscritti nell'elenco pubblico presso l'Autorità per l'informatica nella pubblica amministrazione secondo la vigente normativa in materia di contratti pubblici. In questo caso non vi è l'obbligo dell'iscrizione nel citato elenco pubblico.
2. Per la sottoscrizione di documenti informatici di rilevanza interna, le pubbliche amministrazioni possono emettere certificati di firma digitale secondo regole tecniche diverse da quelle di cui al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999.
3. Per la formazione e la gestione di documenti informatici per i quali non è prevista la sottoscrizione, le pubbliche amministrazioni possono utilizzare sistemi elettronici di identificazione ed autenticazione nell'ambito della propria autonomia organizzativa e dei processi di razionalizzazione.
4. Per la formazione e la sottoscrizione dei documenti informatici, secondo quanto stabilito dal decreto del Presidente della Repubblica 10 novembre 1997 e dalle regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, le pubbliche amministrazioni devono attenersi alle regole di interoperabilità definite dalla circolare AIPA/CR/24 del 19 giugno 2000.

Art. 6

Gestione dei documenti informatici

1. La gestione dei documenti informatici e le attività relative al protocollo informatico sono effettuate secondo i principi stabiliti dal decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 e le relative regole tecniche.

Art. 7

Conservazione dei documenti informatici

1. Per la conservazione e la esibizione dei documenti informatici, avuto riguardo a quanto previsto dall'articolo 6, comma 5, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, e dall'articolo 61 del decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, si applicano le regole tecniche emanate con deliberazione dell'Autorità per l'informatica nella pubblica amministrazione 30 luglio 1998, n. 24, ai sensi dell'art. 2, comma 15, della legge 24 dicembre 1993, n. 537.
2. Per l'estensione della validità del documento informatico si applica l'articolo 60 del decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999.

Art. 8

Trasmissione dei documenti informatici

1. Per la trasmissione dei documenti informatici si applicano le regole tecniche di cui agli articoli 4, 6 e 17 del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428, e successive modificazioni ed integrazioni.
2. Le pubbliche amministrazioni disciplinano autonomamente la trasmissione interna dei documenti informatici con riferimento al proprio ordinamento.

Art. 9

Accesso ai documenti informatici

1. L'accesso ai documenti informatici è regolato dalla legge 7 agosto 1990, n. 241 e successive modificazioni ed integrazioni, anche con riferimento al funzionamento della Rete unitaria delle pubbliche amministrazioni.
2. Le pubbliche amministrazioni regolamentano, con riferimento al proprio ordinamento, l'accesso tramite sistemi informativi automatizzati per le attività di consultazione e di estrazione dei documenti.

Art. 10

Sicurezza dei documenti informatici

1. Le pubbliche amministrazioni predispongono, entro dodici mesi dalla data di entrata in vigore della presente deliberazione, un piano per la sicurezza informatica relativo alla formazione ed alla conservazione dei documenti informatici.
2. Il piano fa parte del manuale di gestione di cui alle regole tecniche emanate ai sensi del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.
3. Il piano considera almeno i seguenti aspetti: analisi dei rischi, politiche di sicurezza, interventi operativi.
4. Il piano è sottoposto a verifica ed aggiornato con cadenza almeno biennale.
5. Le pubbliche amministrazioni adottano le misure minime di sicurezza dei dati personali ai sensi dell'art. 15 della legge 31 dicembre 1996, n. 675, e del relativo regolamento di

attuazione emanato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318.

Roma, 23 novembre 2000

Il Presidente: REY