

Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004

**Regole tecniche per la formazione, la trasmissione, la conservazione, la
duplicazione, la riproduzione e la validazione, anche temporale,
dei documenti informatici.**

(G.U. n.98 del 27 aprile 2004)

Il Presidente del Consiglio dei Ministri

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa e in particolare l'articolo 8, comma 2;

Visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche;

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

Vista la decisione della Commissione europea 14 luglio 2003, relativa alla pubblicazione dei numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata sulla Gazzetta ufficiale dell'Unione Europea L 175/45 del 15 luglio 2003 che induce ad integrare in tal senso le premesse del provvedimento;

Visto il decreto del Presidente del Consiglio dei ministri 9 agosto 2001, con il quale è stata attribuita al Ministro per l'innovazione e le tecnologie, dott. Lucio Stanca, tra l'altro, la delega ad esercitare le funzioni spettanti al Presidente del Consiglio dei ministri nelle materie dell'innovazione tecnologica, dello sviluppo della società dell'informazione, nonché delle connesse innovazioni per le amministrazioni pubbliche;

Sentito il Ministro per la funzione pubblica;

Sentito il Garante per la protezione dei dati personali;

Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, CE attuata con decreto legislativo 23 novembre 2000, n. 427;

DECRETA

**TITOLO I
DISPOSIZIONI GENERALI**

Art. 1

Definizioni

1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute negli articoli 1 e 22 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni. Si intende, inoltre, per:

- a) TESTO UNICO, il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, emanato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
- b) DIPARTIMENTO, il dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri o altro organismo di cui si avvale il Ministro per l'innovazione e le tecnologie;
- c) CHIAVI, la coppia di chiavi asimmetriche come definite all'articolo 22, comma 1, lettera b), del testo unico;
- d) IMPRONTA di una sequenza di simboli binari (*bit*), la sequenza di simboli binari (*bit*) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*;
- e) FUNZIONE DI HASH, una funzione matematica che genera, a partire da una generica sequenza di simboli binari (*bit*), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (*bit*) per le quali la funzione generi impronte uguali;
- f) EVIDENZA INFORMATICA, una sequenza di simboli binari (*bit*) che può essere elaborata da una procedura informatica;
- g) RIFERIMENTO TEMPORALE, informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
- h) VALIDAZIONE TEMPORALE, il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi;
- i) MARCA TEMPORALE, un'evidenza informatica che consente la validazione temporale.

Art. 2

Ambito di applicazione

1. Il presente decreto stabilisce, ai sensi dell'articolo 8, comma 2, del testo unico, le regole tecniche per la generazione, apposizione e verifica delle firme digitali.
2. Le disposizioni di cui al titolo II si applicano ai certificatori che rilasciano al pubblico certificati qualificati ai sensi del testo unico.
3. Ai certificatori accreditati o che intendono accreditarsi ai sensi del testo unico si applicano, oltre a quanto previsto dal comma 2, anche le disposizioni di cui al titolo III.
4. I certificatori accreditati devono disporre di un sistema di validazione temporale conforme alle disposizioni di cui al titolo IV.
5. Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione europea e dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE, è consentito di circolare liberamente nel mercato interno.
6. Le disposizioni di cui al comma 5 si applicano anche agli Stati non appartenenti all'Unione europea con i quali siano stati stipulati specifici accordi di riconoscimento reciproco.

TITOLO II

REGOLE TECNICHE DI BASE

Art. 3

Norme tecniche di riferimento

1. I prodotti di firma digitale e i dispositivi sicuri di firma di cui all'articolo 29-*sexies* del testo unico, devono essere conformi alle norme generalmente riconosciute a livello internazionale o individuate dalla Commissione europea secondo la procedura di cui all'articolo 9 della direttiva 1999/93/CE.
2. Gli algoritmi di generazione e verifica delle firme digitali e le funzioni di *hash* sono individuati ai sensi del comma 1.
3. Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma, non produce gli effetti di cui all'articolo 10, comma 3, del testo unico, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Art. 4

Caratteristiche generali delle chiavi per la creazione e la verifica della firma

1. Una coppia di chiavi per la creazione e la verifica della firma può essere attribuita ad un solo titolare.
2. Se il titolare appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.
3. Se la procedura automatica fa uso di più dispositivi per apporre la firma del medesimo titolare, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo.
4. Ai fini del presente decreto, le chiavi di creazione e verifica della firma ed i correlati servizi, si distinguono secondo le seguenti tipologie:
 - a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
 - b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte o associate ai certificati qualificati, alle liste di revoca (CRL) e sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
 - c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.
5. Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, dal precedente comma 4.
6. In deroga a quanto stabilito al comma 5, le chiavi di certificazione di cui al comma 4, lettera b), possono essere utilizzate per altre finalità previa autorizzazione da parte del Dipartimento.
7. La robustezza delle chiavi deve essere tale da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche.

Art. 5

Generazione delle chiavi

1. La generazione della coppia di chiavi deve essere effettuata mediante dispositivi 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 della coppia di 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.

Art. 6

Modalità di generazione delle chiavi

1. Le chiavi di certificazione possono essere generate esclusivamente dal responsabile del servizio.
2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.
3. La generazione delle chiavi di sottoscrizione effettuata, autonomamente dal titolare, deve avvenire all'interno del dispositivo sicuro per la generazione delle firme, che deve essere rilasciato o indicato dal certificatore.
4. Il certificatore deve assicurarsi che il dispositivo sicuro per la generazione delle firme, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'articolo 29-*sexies* del testo unico e all'articolo 9 del presente decreto.
5. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art. 7

Conservazione delle chiavi

1. È vietata la duplicazione della chiave privata e dei dispositivi che la contengono.
2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate purché ciò avvenga con modalità tali da non ridurre il livello di sicurezza.
3. Il titolare della coppia di chiavi deve:
 - a) conservare con la massima diligenza la chiave privata o 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 separatamente dal dispositivo contenente la chiave;
 - c) richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso.

Art. 8

Generazione delle chiavi al di fuori del dispositivo di firma

1. Se la generazione delle chiavi avviene su un sistema diverso da quello destinato all'uso della chiave privata, il sistema di generazione 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.

Art. 9

Dispositivi sicuri e procedure per la generazione della firma

1. In aggiunta a quanto previsto all'articolo 29-*sexies* del testo unico, la generazione della firma deve avvenire all'interno di un dispositivo sicuro di firma, così che non sia possibile l'intercettazione della chiave privata utilizzata.
2. Il dispositivo sicuro di firma deve poter essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma.
3. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, secondo i criteri indicati all'articolo 53.
4. La personalizzazione del dispositivo sicuro di firma deve almeno garantire:
 - a) l'acquisizione da parte del certificatore dei dati identificativi del dispositivo di firma utilizzato e la loro associazione al titolare;
 - b) la registrazione nel dispositivo di firma del certificato qualificato, relativo alle chiavi di sottoscrizione del titolare.
5. La personalizzazione del dispositivo sicuro di firma può prevedere, per l'utilizzo nelle procedure di verifica della firma, la registrazione, nel dispositivo di firma, del certificato elettronico relativo alla chiave pubblica del certificatore la cui corrispondente privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare;
6. La personalizzazione del dispositivo di firma è registrata nel giornale di controllo.
7. Il certificatore deve adottare, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme, procedure atte ad identificare il titolare di un dispositivo sicuro di firma e dei certificati in esso contenuti.

Art. 10

Verifica delle firme digitali

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

Art. 11

Informazioni riguardanti i certificatori

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi del testo unico devono fornire al dipartimento le seguenti informazioni e documenti:
 - a) dati anagrafici ovvero denominazione o ragione sociale;
 - b) residenza ovvero sede legale;
 - c) sedi operative;
 - d) rappresentante legale;
 - e) certificati delle chiavi di certificazione;
 - f) piano per la sicurezza contenuto in busta sigillata;
 - g) manuale operativo di cui al successivo articolo 38;
 - h) dichiarazione di impegno al rispetto delle disposizioni del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
 - i) dichiarazione di conformità ai requisiti previsti nel presente decreto;
 - l) relazione sulla struttura organizzativa;
 - m) copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.
2. Il Dipartimento rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), d).
3. Restano salve le disposizioni del decreto del Presidente della Repubblica 23 dicembre 1997, n. 522, e successive modificazioni, con riferimento ai compiti di certificazione e di validazione temporale del Centro nazionale per l'informatica nelle pubbliche amministrazioni, in conformità alle disposizioni dei regolamenti previsti dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

Art. 12

Comunicazione tra certificatore e Dipartimento

1. I certificatori che rilasciano al pubblico certificati qualificati devono attenersi alle regole emanate dal Dipartimento per realizzare un sistema di comunicazione sicuro attraverso il quale scambiare le informazioni previste dal presente decreto.

Art. 13

Generazione delle chiavi di certificazione

1. La generazione delle chiavi di certificazione deve avvenire in modo conforme a quanto previsto dal presente Titolo.
2. Per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

3. I valori contenuti nei singoli campi del certificato delle chiavi di certificazione devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

Art. 14

Generazione dei certificati qualificati

1. In aggiunta agli obblighi previsti per il certificatore dall'articolo 29-*bis* del testo unico prima di emettere il certificato qualificato il certificatore deve:
 - a) accertarsi dell'autenticità della richiesta;
 - b) verificare il possesso della chiave privata e il corretto funzionamento della coppia di chiavi.
2. Il certificato qualificato deve essere generato con un sistema conforme a quanto previsto dall'articolo 28.
3. L'emissione dei certificati qualificati deve essere registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione.
4. Il momento della generazione dei certificati deve essere attestato tramite un riferimento temporale.

Art. 15

Informazioni contenute nei certificati qualificati

1. Fatto salvo quanto previsto dall'articolo 27-*bis* del testo unico, i certificati qualificati devono contenere almeno le seguenti informazioni:
 - a) codice identificativo del titolare presso il certificatore;
 - b) tipologia della coppia di chiavi in base all'uso cui sono destinate.
2. Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare della firma elettronica, per legittimare la sottoscrizione del documento informatico, nonché per indicare eventuali funzioni del titolare.
3. I valori contenuti nei singoli campi del certificato qualificato devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.
4. Il certificatore determina il periodo di validità dei certificati qualificati in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati.
5. Il certificatore custodisce le informazioni di cui all'articolo 29-*bis*, comma 2, lettera *m*) del testo unico, per un periodo non inferiore a dieci anni dalla data di scadenza o revoca del certificato qualificato.

Art. 16

Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'articolo 29-*septies* del testo unico, il certificato qualificato deve essere revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma.

2. 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 chiave privata della nuova coppia.
3. I certificati generati secondo quanto previsto dal comma 2 debbono essere inviati al Dipartimento.

Art. 26

Revoca dei certificati relativi a chiavi di certificazione

1. La revoca del certificato relativo ad una coppia di chiavi di certificazione è consentita solo nei seguenti casi:
 - a) compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata.
 - b) guasto del dispositivo di firma;
 - c) cessazione dell'attività.
2. La revoca deve essere notificata entro ventiquattro ore al dipartimento e a tutti i titolari di certificati qualificati firmati con la chiave privata appartenente alla coppia revocata.
3. I certificati qualificati per i quali risulta compromessa la chiave privata con cui sono stati sottoscritti devono essere revocati.

Art. 27

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 qualificati e la gestione del registro dei certificati qualificati, devono essere conformi quanto meno alle specifiche previste dalla classe ITSEC F-C2/E2 o equivalenti.
2. Il requisito di cui al comma 1 non si applica al sistema operativo dei dispositivi di firma.

Art. 28

Sistema di generazione dei certificati qualificati

1. La generazione dei certificati qualificati deve avvenire su un sistema utilizzato esclusivamente per la generazione di certificati, 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 devono essere registrate sul giornale di controllo.

2. È possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1 purché tra loro compatibili; sono in ogni caso compatibili tra loro le funzioni specificate nei sotto indicati 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, sistema di riferimento temporale.

Art. 34

Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'articolo 33 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.

Art. 35

Formato dei certificati qualificati

1. I certificati qualificati e le informazioni relative alle procedure di sospensione e di revoca devono essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni.

Art. 36

Formato della firma

1. Alla firma digitale deve essere allegato il certificato qualificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Art. 37

Codice di emergenza

1. Per ciascun certificato qualificato emesso il certificatore deve fornire al titolare almeno un codice riservato, da utilizzare in caso di emergenza per confermare l'autenticità della eventuale richiesta di sospensione del certificato.
2. In caso di emergenza è possibile richiedere la sospensione immediata di un certificato qualificato utilizzando il codice previsto al comma 1. La richiesta deve essere successivamente confermata utilizzando una delle modalità previste dal certificatore.
3. Il certificatore adotta specifiche misure di sicurezza per assicurare la segretezza del codice di emergenza

4. Le pubbliche amministrazioni possono anche utilizzare come sistemi di validazione temporale:
 - a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'articolo 9 del decreto del Presidente del Consiglio dei ministri, 31 ottobre 2000, pubblicato sulla Gazzetta Ufficiale 21 novembre 2000, n. 272;
 - b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti;
 - c) il riferimento temporale ottenuto attraverso l'utilizzo di posta certificata ai sensi dell'articolo 14 del testo unico.

TITOLO III

ULTERIORI REGOLE PER I CERTIFICATORI ACCREDITATI

Art. 40

Obblighi per i certificatori accreditati

1. Il certificatore deve generare un certificato qualificato per ciascuna delle chiavi di firma elettronica avanzata utilizzate dal dipartimento per la sottoscrizione dell'elenco pubblico dei certificatori e pubblicarlo nel proprio registro dei certificati.
2. Il certificatore garantisce l'interoperabilità del prodotto di verifica di cui all'articolo 10 ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative.
3. Il certificatore deve mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiavi di certificazione di cui all'articolo 41, comma 1, lettera f), che deve rendere accessibile per via telematica.
4. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'articolo 28, comma 1 del testo unico, devono svolgere la propria attività in conformità con quanto previsto dalle regole per il riconoscimento e la verifica del documento elettronico.

Art. 41

Elenco pubblico dei certificatori accreditati

1. L'elenco pubblico dei certificatori accreditati tenuto dal Dipartimento ai sensi del testo unico, contiene per ogni certificatore accreditato le seguenti informazioni:
 - a) denominazione;
 - b) sede legale;
 - c) rappresentante legale;
 - d) nome X.500;
 - e) indirizzo internet;
 - f) lista dei certificati delle chiavi di certificazione;
 - g) manuale operativo;
 - h) data di accreditamento volontario;
 - i) data di cessazione ed eventuale certificatore sostitutivo.

2. L'elenco pubblico è sottoscritto e reso disponibile per via telematica dal Dipartimento.
3. Il Dipartimento provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione e a rendere la stessa disponibile ai certificatori per la pubblicazione ai sensi dell'articolo 40, comma 3.
4. L'elenco pubblico è sottoscritto dal Capo del dipartimento o dal dirigente da lui designato, mediante una firma elettronica avanzata, generata mediante un dispositivo sicuro per la creazione di una firma.
5. Sulla Gazzetta Ufficiale è dato avviso:
 - a) della costituzione dell'elenco di cui al comma 4;
 - b) dell'indicazione del soggetto preposto alla sottoscrizione dell'elenco pubblico di cui al comma 4;
 - c) del valore dei codici identificativi delle chiavi pubbliche relative alle coppie di chiavi utilizzate per la sottoscrizione dell'elenco pubblico, generati attraverso gli algoritmi *dedicated hash-function 3*, corrispondente alla funzione SHA-1 e *dedicated hash-function 1*, corrispondente alla funzione RIPEMD-160, definiti nella norma ISO/IEC 10118-3:1998;
 - d) con almeno novanta giorni di preavviso, della scadenza delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico;
 - e) della revoca delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico sopravvenute per ragioni di sicurezza, ovvero a seguito di sostituzione dei soggetti designati ai sensi della lettera b).
6. Fino alla certificazione delle chiavi da parte del Dipartimento ai sensi dell'articolo 29-*quinquies* del testo unico si utilizzano, per la sottoscrizione dell'elenco pubblico, le chiavi di sottoscrizione di soggetti designati dal Ministro per l'innovazione e le tecnologie.

Art. 42

Rappresentazione del documento informatico

1. Il certificatore deve indicare nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per ottemperare a quanto prescritto dall'articolo 3, comma 3.

Art. 43

Limitazioni d'uso

1. Il certificatore, su richiesta del titolare o del terzo interessato, è tenuto a inserire nel certificato qualificato eventuali limitazioni d'uso.

valutazione E3 e robustezza HIGH dell'ITSEC, o dal livello EAL 4 della norma ISO/IEC 15408 o superiori. Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

4. Il Dipartimento disciplina con circolare il riconoscimento e la verifica del documento elettronico; fino all'emanazione della prima circolare continueranno ad applicarsi le regole vigenti adottate dall'Autorità per l'informatica nelle pubbliche amministrazioni.

Art. 54

Abrogazioni

1. Dall'entrata in vigore del presente decreto è abrogato il decreto del Presidente del Consiglio dei ministri 8 febbraio 1999, recante le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, pubblicato sulla Gazzetta Ufficiale 15 aprile 1999, n. 87.

Roma, 13 gennaio 2004

p. Il Presidente: Stanca

Registrato alla Corte dei conti il 19 marzo 2004

Ministeri istituzionali - Presidenza del Consiglio dei Ministri,
registro n. 3, foglio n. 16