CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

LINEE GUIDA PER LA VIGILANZA SUI CERTIFICATORI QUALIFICATI

(Art. 31 Decreto Legislativo 7 MARZO 2005, N. 82)

V1.2

10 settembre 2008

Ufficio Sicurezza
Centro Nazionale per l'informatica nella Pubblica Amministrazione

Sommario

Capitolo 1

Introduzione

1.1 Premessa

L'articolo 31 del decreto legislativo 7 marzo 2005, n. 82 ("*Il CNIPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e accreditati.*") individua nel Centro nazionale per l'informatica nella pubblica amministrazione l'organismo a cui è affidato il compito di espletare quanto prescritto dai commi 2 e 3 dell'articolo 3 della Direttiva europea 1999/93/CE:

> *"2. [omissis], gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi volti a fornire servizi di certificazione di livello più elevato. Tutte le condizioni relative a tali sistemi devono essere obiettive, trasparenti, proporzionate e non discriminatorie. Gli Stati membri non possono limitare il numero di prestatori di servizi di certificazione accreditati per motivi che rientrano nell'ambito di applicazione della presente direttiva."*
>
> *"3. Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilascia al pubblico certificati qualificati".*

Con il dispositivo giuridico sopra citato il CNIPA è stato quindi designato, anche a livello comunitario (si veda quanto riportato all'indirizzo internet http://europa.eu.int/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#Italy), a operare come l'organismo nazionale di accreditamento e di vigilanza sulle attività svolte dai certificatori qualificati e accreditati.

Per chiarezza di informazione si ricorda che in queste Linee Guida si intendono per "certificatori qualificati" i soggetti che intendono emettere certificati qualificati secondo la Direttiva europea 1999/93/CE, e per "certificatori accreditati" coloro, tra i medesimi certificatori qualificati, che decidono liberamente di sottoporsi ad apposita istruttoria preventiva volta a verificare il possesso in capo agli stessi dei requisiti richiesti dalle norme in materia.

E' quindi possibile che un certificatore qualificato sia anche accreditato, mentre non è possibile il contrario. Nella realtà, poiché lo scambio con le pubbliche amministrazioni di documenti sottoscritti con firma digitale deve far uso di certificati qualificati rilasciati da certificatori accreditati, alla data tutti i certificatori qualificati hanno intrapreso le azioni necessarie per essere anche accreditati.

Inoltre, è opportuno ricordare che tali soggetti non svolgono solo l'attività di certificazione inerente la firma digitale ma anche, ai sensi del regolamento (DPR 117/2004) relativo alla Carta Nazionale dei Servizi (CNS), l'attività di rilascio dei certificati di autenticazione necessari all'emissione di tale smart card.

A parte il rispetto degli obblighi normativi, la vigilanza su tali soggetti è ovviamente fondamentale per l'intero impianto della firma digitale nel nostro Paese e, di conseguenza, per consentire anche il libero scambio di documenti informatici nell'ambito della Comunità Europea e con altre comunità che riconoscano almeno le misure tecniche e organizzative coerenti con la citata Direttiva 1999/93/CE. Difatti, la robustezza degli algoritmi utilizzati, la sicurezza dei dispositivi sicuri per la generazione della firma (smart card), i meccanismi crittografici utilizzati, non potrebbero garantire nulla se il soggetto che certifica la corrispondenza fra una chiave pubblica ed i dati anagrafici del titolare della stessa, ad esempio, non agisse con serietà e competenza, garantendo quindi i richiesti livelli di affidabilità, qualità e sicurezza.

1.2 Obiettivi del documento

L'ampia gamma delle attività svolte dai certificatori, che può comportare il rispetto della normativa anche con soluzioni tecniche differenti, e la doverosa "neutralità" delle norme giuridiche, che correttamente non specificano tutti i requisiti tecnici nei minimi dettagli, rendono necessario definire una base comune di valutazione su cui fondare le operazioni di vigilanza. Questo allo scopo di raggiungere una equanimità nelle valutazioni sul rispetto delle norme da parte dei certificatori.

Il presente documento ha l'obiettivo di indicare, sia ai certificatori soggetti a vigilanza sia a coloro che tale vigilanza espletano tramite verifiche e ispezioni, qui denominati "valutatori", le modalità con cui le operazioni di vigilanza vanno svolte da parte dei "valutatori", e le attività di supporto che i certificatori devono fornire ai medesimi "valutatori" nel corso di tali operazioni.

1.3 Struttura del documento

Le presenti Linee Guida sono strutturate in base allo schema delle Specifiche tecniche ETSI TS 101 456 e del Technical Report ETSI TR 102 437.

Tale scelta è stata fatta in quanto il TS 101 456, per la cui attuazione il TR 102 437 fornisce le Linee guida, è stato redatto dallo European Telecommunications Standards Institute – ETSI – nell'ambito della European Electronic Signature Standardisation Initiative, lanciata nel 1999 su impulso della Commissione Europea con lo scopo di fornire alla Direttiva 1999/93/EC una adeguata base tecnica. In particolare:

1. lo ETSI TS 101 456:
    a. è lo schema di Certificate Policy adottato da un sempre maggior numero di paesi membri della Comunità Europea; esso pertanto costituisce una base comune in tali paesi;
    b. è stato riconosciuto comparabile con la US Federal Bridge CA Certificate Policy, Medium Level, come indicato nello ETSI TR 102 438; come conseguenza un utente di un certificatore europeo che abbia strutturato le proprie Certificate Policy in base allo ETSI TS 101 456 otterrà un più agevole inserimento tra gli utenti di certificatori riconosciuti dallo US Federal Bridge CA del Governo degli USA;
2. lo ETSI TR 102 437 è impostato in base a un documento dello olandese TTP.NL[1] con finalità analoghe a quelle di queste Linee Guida; esso quindi costituisce un fattore di uniformità sicuramente con un altro paese della Unione Europea e sta diventando un sicuro punto di riferimento in questo campo.

Per i motivi precedenti si ritiene che strutturare le presenti Linee Guida in base ai citati ETSI TS 101 456 e TR 102 437 costituisca una valida premessa per il raggiungimento dell'interoperabilità in sede Europea e, almeno per quanto riguarda i certificati qualificati, per una più agevole interazione con le amministrazioni del Governo USA e con i suoi fornitori.

A integrazione di quanto indicato nello ETSI TS 101 456 si è ritenuto opportuno fare riferimento, ove necessario, anche alle specifiche indicate negli standard ISO/IEC comunemente adottati nel campo della sicurezza dei sistemi informatici. In particolare si è fatto riferimento alle indicazioni sulle misure di sicurezza specificate nello ISO/IEC 17799:2005 che sono indicate come "Best practices" per attuare i controlli indicati nello Annex A dello ISO/IEC 27001:2005.

Il documento, quindi, dopo alcuni capitoli introduttivi che riportano il quadro giuridico e tecnico di riferimento e le principali modalità di impostazione delle verifiche, entra nel dettaglio degli specifici aspetti tecnico-giuridici dell'attività di certificazione dedicando a ognuno di essi un capitolo, suddiviso in tre paragrafi:

1. il primo paragrafo indica i dispositivi giuridici che specificamente riguardano l'argomento o gli argomenti a cui il capitolo stesso si rivolge;

[1] TTP.NL è uno schema di accreditamento volontario, nato a seguito di un'iniziativa promossa dal Ministero degli affari economici olandese, che opera sotto la gestione dello Electronic Commerce Platform Netherlands, ECP.NL. Questo schema ha l'obiettivo di valutare la conformità dei certificatori allo ETSI TS 101 456.

2. il secondo indica le attività operative e di supporto che il certificatore deve svolgere per rendere possibile le operazioni di vigilanza;
3. il terzo indica le attività sulle quali si può basare il valutatore nell'operare.

Il documento si conclude con un allegato che riporta l'intero corpus della normativa afferente la firma digitale e le attività di certificazione. Ai singoli articoli e commi dei dispositivi ivi riportati fanno riferimento, anche mediante collegamento ipertestuale, le citazioni riportate nel primo paragrafo di ognuno dei capitoli di cui sopra.

1.4 Termini chiave

In queste Linee Guida vengono utilizzati i seguenti termini chiave con il significato previsto dallo IETF RFC 2119.

Le parole chiave "DEVE" o "DEVONO" o "E' RICHIESTO" stanno a significare che l'oggetto in questione è un requisito assoluto della definizione.

Le parole chiave "NON DEVE" o "NON DEVONO" stanno a significare che l'oggetto in questione è un divieto assoluto per la definizione.

Le parole chiave "DOVREBBE" o "RACCOMANDATO" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di scegliere per un'altra soluzione.

Le parole chiave "NON DOVREBBE" o "NON RACCOMANDATO" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di implementare una soluzione corrispondente.

Le parole chiave "PUO'" o "OPZIONALE" stanno a significare che una specifica è puramente opzionale.

Capitolo 2

Sintesi del quadro normativo di riferimento

2.1 La Direttiva Europea 1999/93/CE

Il 13 dicembre 1999 fu varata la Direttiva 1999/93/CE del Parlamento europeo e del Consiglio relativa ad un quadro comunitario per le firme elettroniche. Tale Direttiva fu pubblicata sulla Gazzetta ufficiale delle Comunità europee il 19 gennaio 2000, data in cui è entrata in vigore.

Questa Direttiva era ovviamente stata preceduta da un periodo di gestazione durato svariati anni, durante i quali si erano già sviluppate le normative al riguardo di alcuni Stati membri della Comunità europea, tra cui l'Italia. E' quindi naturale che la Direttiva abbia tenuto in debito conto almeno i punti qualificanti di queste norme unificando i requisiti che soddisfano le esigenze dei vari Stati membri della Comunità.

2.2 La normativa giuridico-tecnica italiana – breve excursus storico

L'Italia vanta in Europa il primato cronologico del riconoscimento dei documenti elettronici, stabilito all'art. 15 comma 2 della legge 15 marzo 1997, N. 59, pubblicata in Gazzetta ufficiale il 17 marzo 1997 che recita:

> "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni."

Il regolamento di cui parla tale comma fu emesso con il Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 pubblicato sulla Gazzetta ufficiale del 13/3/1998 ("*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59").*

In esso venivano introdotti alcuni concetti sostanzialmente ancora in vigore, a cominciare dalla definizione di documento informatico ("*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"). Vi troviamo infatti, ad esempio:

- Art. 4 comma 1: "*Il documento informatico munito dei requisiti previsti dal presente regolamento soddisfa il requisito legale della forma scritta.*"
- Art. 5 comma 1: "*Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.*"
- Art. 6 comma 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 con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3.*"
- Art. 8 comma 3: "*le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 3:*
  - *a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione dell'attività bancaria, se soggetti privati;*"
- gli obblighi dei titolari e del certificatore (Art. 9);
- eccetera.

Al DPR 513/97 fece seguito il Decreto del Presidente del Consiglio dei ministri del 8 febbraio 1999, pubblicato sulla Gazzetta ufficiale del 15/4/1999 ("*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*"). Anche in esso troviamo sostanzialmente i requisiti di base ancora oggi in vigore, a parte alcuni adeguamenti all'evoluzione della tecnica e della giuridica comunitaria. Vi troviamo infatti la distinzione tra chiavi di certificazione, di sottoscrizione e di marcatura temporale, i requisiti tecnico-organizzativi per la generazione e la conservazione delle chiavi, le caratteristiche di base dei certificati, le specifiche dell'Elenco pubblico del certificatori, ecc.

La Circolare, prevista nel DPCM 8/2/99, per la definizione delle norme per l'accreditamento dei certificatori fu emessa dall'Autorità per l'Informatica nella Pubblica Amministrazione il 26 luglio 1999, con il n. AIPA/CR/22, seguita il 16 febbraio 2001dalla Circolare n. 27 per gli analoghi adempimenti da parte di Pubbliche Amministrazioni.

Il 19 giugno 2000 un'altra Circolare AIPA, con il numero AIPA/CR/24, indicava le norme tecniche da seguire per assicurare l'interoperabilità tra i certificati emessi dai diversi certificatori accreditati, i documenti firmati in base a tali certificati, le liste di revoca, ecc. Va notato che la diffusione della firma digitale raggiunta in Italia si deve in misura rilevante al rispetto di queste norme di interoperabilità.

Nel contempo, il 28/12/2000, era stato promulgato il Decreto del Presidente della Repubblica N. 445 ("*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*), pubblicato in Gazzetta Ufficiale il 20/02/2001, che raccoglieva, unificandoli, tutti i dispositivi giuridici in materia.

Per il recepimento della Direttiva europea 1999/93/CE fu necessario, però, attendere fino al 23 gennaio 2002 quando fu emesso il Decreto legislativo n. 10, pubblicato sulla Gazzetta ufficiale del 15/2/2002.

Alcune cose cambiavano: si colmava quello che agli occhi di qualcuno appariva come un vuoto legislativo, cioè l'esplicito riconoscimento della firma elettronica che oggi chiameremmo non qualificata, si introduceva lo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, ecc.

Conseguentemente veniva aggiornato il DPCM 8/2/99 con l'emissione, il 23/1/2004, del nuovo Decreto Presidente del Consiglio dei Ministri, pubblicato in Gazzetta ufficiale il 27 Aprile 2004 e tutt'ora in vigore, che stabilisce le norme tecniche per i certificatori.

Nel frattempo in Europa, al fine di agevolare lo scambio all'interno della Comunità dei documenti informatici, si erano realizzati gli standard di cui viene dato cenno al Capitolo 3 – Gli standard di riferimento, per cui il CNIPA ritenne opportuno aggiornare i requisiti atti ad agevolare tale interoperabilità, che erano stati indicati nella citata Circolare AIPA/CR/24. Fu così emanata, il 17 febbraio 2005, la Deliberazione n. 4/2005 ("*Regole per il riconoscimento e la verifica del documento informatico."*), pubblicata nella Gazzetta ufficiale il 3 marzo 2005.

L'ultimo tassello della normativa avrebbe potuto essere l'aggiornamento della Circolare AIPA/CR/22, cioè la Circolare CNIPA del 6 settembre 2005, n. 48 (pubblicata nella Gazzetta ufficiale il 13 settembre 2005, n. 213), ma nel frattempo veniva promulgato il Decreto Legislativo n. 82 del 07/03/2005 ("Codice dell'amministrazione digitale"), Pubblicato in Gazzetta Ufficiale il 16/05/2005, successivamente aggiornato da un altro Decreto legislativo, il N. 159 del 4 aprile 2006, pubblicato in Gazzetta Ufficiale il 29 Aprile 2006.

Il Codice dell'Amministrazione Digitale – CAD apporta alcune variazioni alla normativa preesistente, quali l'allungamento a venti anni dei termini per la conservazione della documentazione relativa ai certificati, l'obbligo per il titolare di utilizzare personalmente il dispositivo sicuro di firma, e altri aspetti giuridici del riconoscimento dei vari tipi di firme elettroniche.

Il quadro dei dispositivi giuridici attualmente in vigore, tra quelli indicati sopra, è riportato dal Capitolo 13 al Capitolo 15.

Capitolo 3

Gli standard di riferimento

Gli aspetti tecnici di base della firma digitale sono regolamentati sostanzialmente da due enti internazionali di standardizzazione: lo Internet Engineering Task Force, che rilascia i cosiddetti RFC ormai generalmente riconosciuti come standard de facto anche quando si trovano ancora nella fase di "PROPOSED STANDARD", e lo International Organization for Standardisation / International Electrotechnical Commission (ISO/IEC). Circa quest'ultimo va anche detto che ad esso si devono gli standard oggi generalmente riconosciuti e utilizzati in materia di sicurezza.

In Europa fu poi lanciato nel 2000 lo EESSI che operò avvalendosi dei due enti di standardizzazione europei: ETSI (European Telecomunications Standardisation Institute) e CEN (Comité Européen de Normalisation).

3.1 Standard ISO/IEC

Gli standard ISO/IEC generalmente usati in relazione alla firma digitale sono quelli comunemente noti come appartenenti alla serie X.500, relativi alla gestione della Directory. Essi sono dapprima emessi come raccomandazioni dallo ITU-T (International Telecommunication Union), che è l'agenzia delle Nazioni Unite specializzata nel campo delle telecomunicazioni, e successivamente recepiti come veri e propri standard dallo ISO/IEC. Quest'ultimo li pubblica con propri identificativi nell'ambito della famiglia degli standard ISO/IEC 9594 il cui titolo generale è: "Information technology — Open Systems Interconnection — The Directory".

I componenti della famiglia 9594 sono attualmente i seguenti:

— Part 1: Overview of concepts, models and services

— Part 2: Models

— Part 3: Abstract service definition

— Part 4: Procedures for distributed operation

— Part 5: Protocol specifications

— Part 6: Selected attribute types

— Part 7: Selected object classes

— Part 8: Public-key and attribute certificate frameworks

— Part 9: Replication

— Part 10: Use of systems management for administration of the Directory

Altri standard ISO/IEC, per dir così, "di contorno" alla serie 9594 sono gli standard relativi alla certificazione di sicurezza di dispositivi quali ad esempio quelli di firma (ISO/IEC 15408), agli algoritmi crittografici (ISO/IEC 10118), a politiche di certificazione in determinate aree di business quali ad esempio quelli finanziari (ISO 21188), ecc.

Infine va ricordato l'insieme di standard relativi alle tecniche di sicurezza che riguardano gli "Information security management systems", riunite nella famiglia della serie 27000, nella quale confluirà anche l'attuale ISO/IEC 17799, derivato dal BS 7799-1.

3.2 IETF

La Internet Engineering Task Force si auto definisce: "un'ampia e aperta comunità internazionale di progettisti, operatori, fornitori e ricercatori nel campo delle reti.".

Essa si articola in numerosissimi gruppi di lavoro (Working Group) organizzati in otto aree di interesse. In una di esse (Security Area) operano i due Working Group (WG) di maggior interesse per la firma digitale: il pkix – Public-Key Infrastructure (X.509) e lo smime – S/MIME Mail Security.

Un elenco completo degli RFC prodotti da questi due WG sarebbe eccessivamente lungo, ci si limita pertanto ad elencarne di seguito i principali, tra quelli che maggiormente si riflettono nell'area della firma digitale.

Nota: l'elenco completo degli RFC emessi, comprendente i collegamenti ipertestuali ai singoli RFC, si può reperire all'indirizzo internet: http://rfc.net/rfc-index.html.

3.2.1 Working Group Public-Key Infrastructure (X.509) (pkix)

RFC 2560 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

RFC 2797 – Certificate Management Messages over CMS

RFC 3161 – Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)

RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile

RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile

RFC 3628 – Policy Requirements for Time-Stamping Authorities (derivato dallo ETSI TS 102 023)

RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocols

RFC 4211 – Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

RFC 4325 – Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension

3.2.2 Working Group S/MIME Mail Security

RFC 3125 – Electronic Signature Policies (derivato dallo ETSI TS 101 733)

RFC 3126 – Electronic Signature Formats for long term electronic signatures (derivato dallo ETSI TS 101 733)

RFC 3370 – Cryptographic Message Syntax (CMS) Algorithms

RFC 3852 – Cryptographic Message Syntax (CMS)

3.3 EESSI

Alla fine del 1998, mentre era ancora in gestazione quella che poi diventò la Direttiva 1999/93/CE, la Commissione Europea chiese allo ICTSB (Information and Communication Technology Standards Board) di valutare se gli standard allora esistenti fornivano alla imminente Direttiva una adeguata base tecnologica da assicurarne l'effettiva applicabilità.

Il 24/2/1999 venne lanciata la European Electronic Signature Standardisation Initiative, che, dopo una iniziale disamina dello stato dell'arte, raccomandò lo sviluppo di standard integrativi a quelli ISO e IETF allo scopo precipuo quello di soddisfare i requisiti posti dalla Direttiva stessa.

Lo ICTSB quindi designò lo ETSI (European Telecomunications Standards Institute) e il CEN (Comité Européen de Normalisation) a sviluppare tali standard integrativi. Nell'ottobre 2004, avendo lo EESSI adempiuto al proprio mandato completando lo sviluppo degli standard la cui necessità era stata individuata nel 1999, lo ICTSB decise di chiuderlo.

Si ricorda che il 14/7/2003 la Commissione europea decise che alcuni degli standard sviluppati in seno allo EESSI, e cioè quelli relativi ai dispositivi di firma e alle caratteristiche di affidabilità dei sistemi utilizzati dai certificatori, andassero indicati come "norme generalmente riconosciute relative a prodotti di firma elettronica conformemente alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio." Questa Decisione fu pubblicata il 15/7/2003 nella Gazzetta ufficiale della Comunità europea

Il Gruppo di lavoro E-sign del CEN terminò la sua attività nel 2003, come pianificato, ma altri Technical Committee del CEN curano la manutenzione dei documenti da esso prodotti e il prosieguo di alcuni di essi ad acquisire lo status di European Norm (EN).

Il Technical Body Electronic Signature and Infrastructures (ESI) dello ETSI invece prosegue tuttora nello sviluppo di ulteriori specifiche, che si stanno adesso orientando verso la parte applicativa della firma elettronica, nella manutenzione dei documenti prodotti e nell'ottenere un mutuo riconoscimento con quelli di altri organismi (quale lo USA Federal PKI).

Anche in questo caso l'elenco di tutti i documenti prodotti dallo EESSI e successivamente dallo ETSI ESI sarebbe eccessivamente lungo. Se ne elencano, quindi, di seguito i principali ai fini della realtà italiana.

3.3.1 CEN E-sign WS

CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)

CWA 14167-3: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

CWA 14167-4: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

CWA 14169: Secure Signature-creation devices "EAL 4+"

CWA 14170: Security requirements for signature creation applications

CWA 14171: General guidelines for electronic signature verification

CWA 14890-1:Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

CWA 14890-2:Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

L'elenco completo delle pubblicazioni prodotte da questo Workshop si può ottenere all'indirizzo internet: http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.

3.3.2 ETSI ESI

ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates

ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 861: Time stamping profile

ETSI TS 101 862: Qualified certificate profile

ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI);Policy requirements for time-stamping authorities

ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2: Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices

ETSI TS 102 231: Provision of harmonized Trust-service status information

ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

ETSI TR 102 437: Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)

L'elenco completo delle pubblicazioni prodotte da questo Technical Body si può ottenere all'indirizzo internet: http://pda.etsi.org/pda/queryform.asp, indicando "ESI" nel campo "Search for" e selezionando la scelta Technical Body Name nell'opzione "Search in…".

3.4 ISO/IEC 17799 e 27001

Al British Standards Institute – BSI – va riconosciuto il merito di avere, molto tempo fa, avvertito l'esigenza di definire una "paradigma" di sicurezza per i sistemi informativi e di aver consolidato tale sensibilità in quello che è poi diventato uno standard, prima de facto e poi de jure: il BS 7799.

Nel 1995 ne fu pubblicata la prima versione che, sia pure impostata sulla normativa giuridica britannica, dava indicazioni su come costituire quello che ormai è noto come Information Security Management System – ISMS.

Una volta date le indicazioni era necessario realizzare uno strumento che consentisse una uniformità di valutazione del loro livello di realizzazione. Nel febbraio 1998 il BSI pubblicò quello che divenne il BS 7799-2, cioè la guida alla valutazione (e anche alla certificazione formale) dello ISMS di un'organizzazione o di una sua parte. Il BS 7799-2, infatti, indicava i requisiti per realizzare e gestire un Information Security Management System, specificando i controlli di sicurezza da attuare a seconda delle necessità.

Da allora queste due parti del BS 7799 si sono evolute. La parte 1 è stata formalizzata nel 2000 come standard ISO/IEC 17799, per essere poi aggiornata nel 2005 e inserita, entro la prima metà del 2007, nella famiglia degli standard di sicurezza ISO/IEC 27000 come ISO/IEC 27002. La parte 2 è stata recepita nel 2005 come standard ISO/IEC 27001.

Si può quindi affermare che questi due standard di sicurezza siano ormai divenuti un punto di riferimento con cui realizzare prima e misurare poi un ISMS, rendendone possibile anche la certificazione di conformità allo standard.

Capitolo 4

Definizioni e Abbreviazioni

4.1 Definizioni

Asset	Risorse materiali e immateriali del certificatore correlate con la fornitura dei suoi servizi. Nota 1: Esempi di asset materiali sono i locali, i sistemi, i dispositivi sicuri di firma. Esempi di asset immateriali sono le informazioni e l'immagine aziendale. Nota 2: La presente definizione è più dettagliata rispetto a quella datane dallo standard ISO 13335: 2004, "anything that has value to the organization", in quanto è più focalizzata alle attività di certificazione.
Auto-certificato	Certificato relativo a una coppia di chiavi di certificazione sottoscritto con la chiave privata della coppia cui il certificato si riferisce.
Datakey	Dispositivi crittografici (usualmente smart card o dispositivi USB) contenenti le chiavi o loro parti (in questo secondo caso normalmente con modalità di secret sharing come definito da Blakley o da Shamir – vedi Bibliografia) con cui attivare un dispositivo crittografico.
Dispositivo sicuro di firma	Apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'Allegato III della Direttiva 1999/93/CE

Hardware Security Module	Modulo crittografico hardware in grado di generare e/o custodire e utilizzare le chiavi private di firma impiegate dal certificatore per apporre la propria firma ai certificati qualificati e alle marche temporali allo scopo di assicurarne autenticità e integrità nel tempo.
Incidente di sicurezza	Un singolo evento inatteso o indesiderato, o una serie di tali eventi, correlato con la sicurezza delle informazioni che abbia una non trascurabile probabilità di compromettere le operazioni di business e di minacciare la sicurezza delle informazioni [ISO/IEC TR 18044:2004]
Information Security Management System	La parte dell'intero sistema di gestione che, in base a una valutazione dei rischi, definisca, realizzi, renda operativa, controlli, sottoponga a revisione, mantenga aggiornata e migliori la sicurezza delle informazioni. Nota: il sistema di gestione comprende strutture organizzative, norme, attività di pianificazione, responsabilità, modalità operative, procedure, processi e risorse. (Traduzione informale dallo ISO/IEC 27001:2005.)
Key escrow	Deposito della chiave privata presso il certificatore o altro ente affidabile in maniera da consentirne a persone autorizzate il recupero in chiaro mediante informazioni in possesso di una o più parti.
Marca temporale	Evidenza informatica che consente la validazione temporale;
Terzo interessato	Persona fisica o giuridica, o suo rappresentante, responsabile nei confronti del certificatore della gestione dei certificati di uno o più titolari che ad essa fanno riferimento
Time Stamping Authority	Ente affidabile che emette TST avvalendosi di sistemi appositi detti TSS
Time Stamp Server	Sistema di cui si avvale un certificatore, operante come TSA, per emettere TST
Time Stamp Token	Marca temporale
Time Stamping Unit	Insieme di hardware e software, facente parte di un Time Stamp Server e da esso gestito in maniera esclusiva per firmare TST, che dispone di un solo dispositivo di firma il quale utilizza una sola coppia di chiavi di firma per volta
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
Valutatore	Il team di valutazione nel suo complesso o i suoi singoli componenti.
Verbale	Qualsiasi documento attestante l'avvenuta effettuazione di procedure, attività, ispezioni, ecc.

4.2 Abbreviazioni

CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
HSM	Hardware Security Module
ISMS	Information Security Management System
TSA	Time Stamping Authority
TSS	Time Stamp Server
TST	Time Stamp Token
TSU	Time Stamping Unit

Capitolo 5

Riferimenti

Circolare CNIPA 48/2005	Circolare 6 settembre 2005, n. 48 – Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
Codice Amministrazione Digitale	Si veda: "Dlgs 82/2005"
Deliberazione CNIPA 4/2005	Deliberazione 17 febbraio 2005 n. 4 – Regole per il riconoscimento e la verifica del documento informatico.
Deliberazione CNIPA 11/2004	Deliberazione N. 11 - 19 febbraio 2004 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
Direttiva 1999/93/CE	Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche
Dlgs 196/2003	Decreto Legislativo del 30/6/2003 n. 196; Codice in materia di protezione dei dati personali
Dlgs 82/2005	Decreto Legislativo del 07/03/2005 n. 82; Codice dell'amministrazione digitale, come modificato dal Decreto legislativo No 159 del 4 aprile 2006.
DPCM 13/1/2004	Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 recante regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.
DPR 445/2000	Decreto del Presidente della Repubblica del 28/12/2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
ETSI TS 101 456	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
ETSI TS 101 861	Time stamping profile
ETSI TS 101 862	Qualified Certificate Profile
ETSI TS 102 176-1	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
ETSI TR 102 437	Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)
ETSI TR 102 438	Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)
ETSI TS 102 280	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels

IETF RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
IETF RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocols (CMP)
ISO/IEC 9594-8: 2001	Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks – Fourth edition 2001-08-01
ISO/IEC 17799: 2005	Information technology — Security techniques — Code of practice for information security management
ISO/IEC 27001: 2005	Information technology — Security techniques — Information security management systems — Requirements
NIST SP 800-57	NIST Special Publication 800-57; May, 2006; Recommendation for Key Management – Part 1: General
Testo Unico	Si veda: "DPR 445/2000"

Capitolo 6

Le modalità di verifica

6.1 Il certificatore

Esibisce documentazione (ivi inclusi, ove del caso, i log di sistema e delle applicazioni) atta a dimostrare il rispetto dei requisiti di legge e di altri requisiti di sicurezza, in conformità con gli standard comunemente adottati, in particolare con gli standard prodotti da ETSI e da ISO/IEC (si veda al Capitolo 3 "Gli standard di riferimento"). Per la maggior parte di essi le modalità specifiche di esibizione della documentazione sono indicate nei singoli capitoli.

Esibisce i verbali di ispezioni effettuate, in conformità con le proprie procedure interne e con frequenza adeguata, presso le proprie sedi e presso le sedi dei fornitori da cui risulti il rispetto degli obblighi.

Nota: sono da ritenersi adeguate frequenze di ispezioni paragonabili alle seguenti:

- mensile: verifiche di:
  - integrità e contenuto del giornale di controllo;
  - esattezza dell'inventario dei dispositivi di firma;
- semestrale: verifiche di:
  - corrispondenza della effettiva configurazione dei sistemi (HW e SW, di PKI, firewall, IDS) con quanto formalizzato e custodito dalla funzione aziendale a ciò deputata;
  - conformità alle procedure delle prassi utilizzate dagli addetti per quanto riguarda le operazioni di:

  - controllo accessi fisici ove non siano utilizzati dispositivi che registrino automaticamente sul giornale di controllo,
  - conservazione della documentazione di registrazione dei titolari, e di revoca e sospensione dei relativi certificati,
  - rispetto delle misure di sicurezza sulla privacy imposte dal Dlgs 196/2003 e successive modificazioni e integrazioni,
  - congruenza tra i dati presenti nella sede principale e in quelle di disaster recovery o di conservazione delle copie di sicurezza;
- annuale: verifiche di:
  - rispetto delle altre procedure utilizzate nell'attività di certificazione;
  - funzionalità della procedura di disaster recovery.

Esibisce verbali di prove di restart dei sistemi e del recupero di dati dai siti di back up.

Esibisce evidenza che a fronte di situazioni riscontrate non in rispondenza con quanto atteso siano state intraprese azioni correttive atte a evitare per il futuro il ripetersi delle medesime, o di analoghe, situazioni.

Qualora da ispezioni effettuate presso fornitori di servizi affidati in outsourcing siano risultate situazioni non in rispondenza con le condizioni contrattuali, esibisce evidenza che sono state intraprese nei confronti dei fornitori le azioni correttive previste dagli accordi stessi atte a evitare per il futuro il ripetersi delle medesime, o di analoghe, situazioni.

Conformemente con la "*dichiarazione di disponibilità a consentire l'accesso di incaricati del CNIPA presso le strutture dedicate alle operazioni di certificazione, al fine di potere verificare la permanenza dei requisiti tecnico-organizzativi documentati all'atto della presentazione della domanda*" depositata presso il CNIPA, garantisce al team di valutazione l'accesso, nel rispetto delle misure di sicurezza indicate nel Piano per la Sicurezza, ai sistemi e locali utilizzati per la fornitura dei servizi di certificazione, anche se di pertinenza di suoi fornitori.

Ove richiesto dal valutatore, esegue specifiche procedure.

Mette a disposizione del valutatore un numero sufficiente di adeguate postazioni di lavoro dotate dei necessari servizi: accesso a internet, alimentazione elettrica, ecc.

6.2 Il valutatore

Nell'analisi delle misure di sicurezza e delle procedure operative adottate dal certificatore il valutatore presumerà che esse siano state impostate in base allo standard ISO/IEC 17799. Qualora il certificatore abbia adottato criteri diversi, sarà sua cura informarne il CNIPA all'atto della informativa della ispezione.

Il team di valutazione nel suo complesso:

1. anteriormente all'ispezione:
   a. prende visione della documentazione depositata presso CNIPA all'atto della richiesta di accreditamento, in conformità con la Circolare CNIPA n. 48 del 2005 o analoghe circolari precedenti, o di eventuali suoi aggiornamenti depositati successivamente, con l'eccezione delle informazioni di cui all'art. 30 del DPCM 13/1/2004, comma 1, lettere b), c) e d) del Piano per la sicurezza che verranno esaminate solo in caso di contestazioni;
   b. verifica che il Manuale Operativo pubblicato presso il sito del certificatore sia il medesimo pubblicato sul sito del CNIPA;
   c. prende visione di Certificate Policy, Certification Practice Statement, Disclosure Statements, ecc. il cui utilizzo è indicato nei certificati emessi dal certificatore;
   d. prende atto delle eventuali autorizzazioni rilasciate da CNIPA all'utilizzo delle chiavi di certificazione dei certificati qualificati per altri usi;

e. acquisisce conoscenza di quali siano le sedi utilizzate dal certificatore come sedi di conservazione delle copie di scorta, come sedi di disaster recovery, o come altre sedi utilizzate per la erogazione dei servizi di certificazione;

f. nel caso in cui il certificatore si avvalga di fornitori per tutti i servizi di certificazione o per loro parte:

   i. acquisisce dal certificatore evidenza che detti fornitori siano adeguatamente formati sulle attività loro demandate.

2. durante l'ispezione, in base a quanto indicato in queste Linee Guida:

   a. verifica, eventualmente a campione:

      i. l'esistenza della documentazione indicata nei vari paragrafi e, ove del caso, la sua rispondenza ai relativi obiettivi;

      ii. che i verbali più recenti si riferiscano a ispezioni effettuate dal certificatore nel rispetto delle proprie procedure, sia al proprio interno sia presso eventuali fornitori, eseguite entro e non oltre il periodo previsto nelle stesse;

      iii. che, ove dalle ispezioni risultino situazioni di non conformità con le procedure, siano state prese azioni correttive atte a evitare per il futuro il ripetersi delle medesime, o analoghe, situazioni;

   b. effettua, eventualmente a campione, i sopralluoghi e gli altri controlli indicati in queste Linee Guida;

   c. può effettuare altri sopralluoghi e controlli, sia tra quelli indicati come facoltativi, sia altri che a suo giudizio siano utili ai fini della valutazione;

   d. può richiedere, onde effettuare le verifiche ritenute necessarie, l'esecuzione delle procedure relative al rilascio di certificati e dei relativi dispositivi sicuri di firma, e alle successive sospensioni e revoche. Questi certificati e dispositivi possono essere utilizzati ai soli fini dell'ispezione e al termine della stessa i dispositivi saranno restituiti e i relativi certificati ancora in vigore saranno revocati.

Verifica che dai verbali di esecuzione delle procedure risulti il rispetto delle medesime.

Verifica le risultanze dei verbali di auditing, siano essi interni o esterni, e, nel caso in cui in tali verbali segnalino problemi, vulnerabilità, mancato rispetto delle procedure, ecc., verifica se a tali segnalazioni siano seguiti interventi correttivi.

Nota1: Le valutazioni delle verifiche, indicate nelle presenti Linee Guida, sulle misure di sicurezza e operative, sulla consistenza e preparazione del personale, sui dispositivi di sicurezza impiegati, saranno fatte sulla base dei documenti in vigore depositati presso CNIPA, anche nel caso in cui versioni più recenti siano esibite dal Certificatore.

Nota 2: La valutazione di vigilanza sui certificatori qualificati non entra nel merito della adeguatezza delle procedure a rispettare le norme di cui al Dlgs 196/2003, ma si limita a verificarne l'esistenza e l'applicazione.

6.3 Modalità dell'ispezione

La data di inizio dell'ispezione viene comunicata da parte di CNIPA al certificatore nella persona del Responsabile delle verifiche e ispezioni, come da DPCM 13/1/2004, art. 33 comma 1 lettera l), con un preavviso minimo di 48 ore.

Il momento dell'inizio dell'ispezione è quindi ufficializzato in un incontro del valutatore con il Responsabile delle verifiche e delle ispezioni del Certificatore, o con persona da lui formalmente incaricata, e con la Direzione Aziendale.

La conclusione dell'ispezione può essere ufficializzata sia in un analogo incontro con il medesimo Responsabile, o con persona da lui formalmente incaricata, sia con una comunicazione del valutatore allo stesso Responsabile, inoltrata per posta ordinaria o per Posta Elettronica Certificata.

Questi due momenti vengono indicati dal valutatore nel verbale dell'ispezione. Il verbale viene controfirmato dal Responsabile delle verifiche e delle ispezioni o da persona da lui formalmente incaricata.

Il valutatore baserà le proprie ispezioni sulla verifica del rispetto di quanto indicato nel Manuale Operativo e nel Piano per la Sicurezza del certificatore, con l'eccezione di quanto indicato all'art. 30 del DPCM 13/1/2004, comma 1, lettere b), c) e d) che verranno esaminate solo in caso di contestazioni, e sulle altre disposizioni indicate nelle presenti Linee Guida.

Altri documenti di riferimento per la conduzione delle valutazioni sono i seguenti documenti citati al capitolo Capitolo 5 – Riferimenti

- ISO/IEC 17799,
- ISO/IEC 27001,
- ETSI TS 101 456.

6.4 Procedure e documentazione del certificatore

Le procedure e la documentazione del certificatore a cui si fa riferimento nei vari capitoli di queste Linee guida devono essere predisposte in conformità con quanto indicato al paragrafo "Normativa" del rispettivo capitolo. Ove in tale paragrafo non siano indicate specifiche norme giuridiche, vengono comunque fornite precise indicazioni su misure di sicurezza che devono essere rispettate nelle procedure in questione.

Tali procedure e tale documentazione possono essere conservate, in tutto o in parte, nel rispetto della normativa vigente (Dlgs 82/2005 art. 22 comma 3 e art. 23 commi 4 e 5, Deliberazione CNIPA 11/2004). In tal caso il valutatore prende atto della relativa dichiarazione del certificatore.

6.5 Verbali

I verbali indicati ai paragrafi seguenti possono essere conservati con modalità informatica, nel rispetto della normativa in vigore (Dlgs 82/2005 art. 22 comma 3 e art. 23 commi 4 e 5, Deliberazione CNIPA 11/2004). In tal caso il valutatore prende atto della relativa dichiarazione del certificatore.

6.5.1 Verbali di auditing

Il certificatore esibisce sempre i verbali di auditing interno ed esterno che attestino la corretta esecuzione delle sue attività di certificazione. Il valutatore verifica che tali verbali esistano e che attestino la correttezza di quanto verificato dall'auditor o dall'ispettore specifico; può verificarne a campione l'autenticità.

6.5.2 Verbali interni

In vari capitoli delle presenti Linee Guida si fa inoltre riferimento a verbali redatti dal certificatore in relazione all'esecuzione di procedure rilevanti ai fini della sicurezza. Ciascuno di questi verbali deve essere redatto in modo formale sotto il controllo della funzione adeguata al caso, ad esempio del Responsabile della Sicurezza o dell'Auditing, e conservato almeno dalla stessa funzione.

Il valutatore:

1. può chiedere l'esibizione di tali verbali;
2. può effettuare verifiche atte a riscontrare la veridicità dei verbali esibiti.

6.6 Dotazione dei valutatori

Il valutatore dispone di propri strumenti, messi a disposizione dal CNIPA, per la verifica del contenuto dei giornali di controllo, dei registri delle marche temporali, ecc.

Capitolo 7

Gestione delle chiavi

7.1 Sistema di generazione dei certificati e relativi locali

Finalità: il certificatore deve garantire che le chiavi di certificazione siano generate in un ambiente sicuro.

7.1.1 Normativa

DPCM 13/1/2004

Art. 28. Sistema di generazione dei certificati qualificati.

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

n) modalità di tenuta del giornale di controllo;

7.1.2 Il certificatore

1. Esibisce la procedura per l'accesso ai locali del sistema di generazione dei certificati, da cui risulti il rispetto dell'art. 28 del DPCM 13/1/2004.

   Nota 1: nel caso in cui i sistemi per i servizi di certificazione siano collocati in locali adeguatamente protetti ma condivisi con altri sistemi destinati ad usi differenti, il certificatore deve provvedere a isolare e proteggere con strutture fisiche i sistemi destinati ai servizi di certificazione, impedendo accessi indebiti; l'accesso alle medesime strutture, che devono poter ospitare contemporaneamente gli addetti previsti per le varie funzioni, deve essere limitato alle sole persone autorizzate di cui saranno registrati sul giornale di controllo ingresso e uscita; l'alimentazione elettrica, le connessioni di rete, eventuali tubature, ecc. devono essere protette; inoltre il certificatore deve:

   a. rendere invisibile dall'esterno quanto presentato su eventuali schermi video ed altri display relativi ai servizi in questione;

   b. formalizzare e rendere operative security policy opportune che richiedano una verifica periodica e, ove necessario, estemporanea dell'integrità delle strutture fisiche di protezione dei sistemi di certificazione;

c. verbalizzare l'esecuzione delle procedure connesse ai servizi di certificazione nel rispetto di tali security policy.

2. Esibisce documentazione che riporti le autorizzazioni del personale ad accedere ai locali ove sono installati i sistemi per la generazione dei certificati e ad operarvi.
3. Consente l'accesso ai locali del sistema di generazione dei certificati al valutatore accompagnato da personale autorizzato, nel rispetto delle misure di sicurezza indicate nel Piano per la sicurezza.
4. Consente al valutatore l'accesso in sola lettura al giornale di controllo, nel quale possano rilevarsi gli accessi ai locali del sistema di generazione dei certificati, ivi compreso anche l'accesso del valutatore stesso, e l'inizio e la fine delle sessioni di lavoro.

7.1.3 Il valutatore

1. Verifica che le modalità di tenuta del giornale di controllo siano conformi con quanto esposto nella dichiarazione presentata dal certificatore in ottemperanza al disposto del punto n) della Circolare CNIPA 48/2005.
2. Verifica che nel giornale di controllo risultino le entrate e le uscite dai locali del personale, tra cui anche quelle del valutatore stesso, e l'accesso ai sistemi.

   Nota: si veda anche quanto indicato nella Nota 1: del paragrafo 7.1.2.
3. Verifica che nel giornale di controllo risultino le attivazioni e le chiusure delle applicazioni e chi le ha innescate.
4. Verifica che le persone che hanno acceduto ai locali in questione e che abbiano attivato / disattivato le applicazioni siano state debitamente e preventivamente autorizzate.
5. Verifica di persona l'impossibilità di accedere a locali, sistemi e applicazioni in questione se non a seguito di controllo accessi fisici e/o logici.
6. Verifica, con l'ausilio del personale autorizzato, che sul sistema di generazione dei certificati non operino altre applicazioni.
7. Verifica che i locali ove si trovano i sistemi per la generazione dei certificati presentino caratteristiche costruttive sicure, ad esempio che gli ingressi controllati non possano restare indefinitamente aperti senza allarme, cosa che potrebbe consentire l'accesso a personale non autorizzato, che non sia possibile distinguere dall'esterno quanto viene presentato sugli schermi video, che vi sia un impianto di anti-incendio, ecc.

7.2 Generazione delle chiavi del certificatore

Finalità: il certificatore deve garantire che le chiavi di certificazione siano generate sotto adeguato controllo.

7.2.1 Normativa

DPCM 13/1/2004

Art. 5. Generazione delle chiavi.

Art. 6. Modalità di generazione delle chiavi. – comma 1

Art. 9. Dispositivi sicuri e procedure per la generazione della firma. – commi 1,2,3

Art. 13. Generazione delle chiavi di certificazione.

Art. 27. Requisiti di sicurezza dei sistemi operativi. – comma 1

Art. 53. Norme transitorie. – commi 1,2,3

7.2.2 Il certificatore

1. Esibisce la procedura, redatta in dettaglio, per la generazione della coppia di chiavi di certificazione prevista dall'art. 5, comma 1, del DPCM 13/1/2004, da cui risulti il rispetto degli art. 6, comma 1, e 13 del medesimo DPCM, e i relativi verbali di esecuzione.
2. Esibisce documentazione attestante la rispondenza di quanto da esso utilizzato per la generazione delle coppie di chiavi di certificazione e per la sottoscrizione dei certificati ai requisiti del DPCM 13/1/2004:
    a. per quanto riguarda i dispositivi: ai criteri di sicurezza indicati all'art. 53, comma 3 e successive modificazioni e integrazioni;
    b. per quanto riguarda i sistemi operativi dei sistemi: ai criteri di sicurezza indicati all'art. 27, comma 1.
3. Esibisce evidenza che le funzioni della procedura di cui al punto 1 assicurino il rispetto delle politiche di sicurezza previste dall'Obiettivo di sicurezza (Security Target) o dal Protection Profile del dispositivo di firma, con particolare attenzione al rispetto della procedura di installazione del dispositivo, alla riservatezza delle chiavi generate e alla riservatezza dei dati per l'autenticazione al dispositivo stesso.
4. Esibisce evidenza dell'utilizzo degli algoritmi indicati all'art. 53 del DPCM 13/1/2004.

    Nota: Nella specifica pubblica ETSI TS 102 176-1, section 6.2.2.1, si evidenzia che "si può usare un esponente basso (per esempio = 3) qualora le esigenze di prestazione siano critiche, altrimenti si RACCOMANDA e $\geq 2^{16}+1$"[2]. Inoltre, sia in considerazione degli studi nell'ambito della criptoanalisi sia per analogia con le specifiche tecniche del tachigrafo[3], si RACCOMANDA di usare esponenti che rispettino anche $e \leq 2^{64}-1$.

7.2.3 Il valutatore

1. Verifica che i verbali della generazione della coppia di chiavi di certificazione, previsti dal punto n. 1 del precedente paragrafo 7.2.2, rispondano a quanto indicato nel Piano per la sicurezza.
2. Della documentazione di cui al punto 2 del paragrafo 7.2.2:
    a. verifica l'esistenza;
    b. verifica l'autenticità.
3. Verifica, in base all'evidenza fornita come indicato ai punti 3 e 4 del paragrafo 7.2.2:
    a. che il verbale della procedura citata al precedente punto 1 rispetti le politiche di sicurezza previste dall'Obiettivo di sicurezza (Security Target) del dispositivo di firma.
    b. che siano utilizzati algoritmi previsti dal DPCM 13/1/2004.

7.3 Contenuto dei certificati di certificazione

Finalità: il certificatore deve garantire che i certificati da esso emessi per le proprie chiavi di certificazione contengano le informazioni previste.

7.3.1 Normativa

DPCM 13/1/2004

[2] "A small public exponent (e.g. e = 3) MAY be used if performance is critical, otherwise e $\geq 2^{16}+1$ is RECOMMENDED."

[3] EUROPEAN COMMISSION JOINT RESEARCH CENTRE – Digital Tachograph System European Root Policy – http://dtc.jrc.it/docs/SPI0416.pdf

Art. 13. Generazione delle chiavi di certificazione. – commi 2,3

Deliberazione CNIPA 4/2005

Art. 5. Profilo dei certificati di certificazione e marcatura temporale – comma 1

Art. 6. Uso delle estensioni nei certificati di certificazione – commi 1, 2

7.3.2 Il certificatore

1. Qualora il campo subjectKeyIdentifier contenga un valore keyIdentifier non calcolato conformemente con la specifica pubblica IETF RFC 3280 il certificatore esibisce documentazione che fornisca adeguata motivazione per aver deviato da tale indicazione.

   Nota: come richiesto nello RFC 3280 il valore keyIdentifier DOVREBBE (SHOULD) essere ottenuto dalla rispettiva chiave pubblica tramite algoritmo di hashing SHA-1 oppure tramite un sistema che assicuri valori unici.

7.3.3 Il valutatore

1. Verifica la rispondenza dei certificati di certificazione ai requisiti di cui alle regole tecniche e di interoperabilità in vigore al momento della generazione del certificato.
2. Qualora il campo subjectKeyIdentifier contenga un valore keyIdentifier non calcolato conformemente con la specifica pubblica IETF RFC 3280 verifica che la documentazione esibita dal certificatore fornisca adeguata motivazione per aver deviato da tale indicazione.

7.4 Sostituzione delle chiavi del certificatore

Finalità: il certificatore deve garantire che le chiavi di certificazione siano sostituite con anticipo e con modalità tali da consentire agli utenti continuità di servizio e la possibilità di verificare la validità dei certificati emessi anche con le coppie di chiavi precedenti.

7.4.1 Normativa

DPCM 13/1/2004

Art. 25. Sostituzione delle chiavi di certificazione.

7.4.2 Il certificatore

1. Esibisce, a integrazione di quanto indicato eventualmente nel Piano per la Sicurezza, una procedura operativa che preveda la realizzazione di quanto indicato all'Art. 25 del DPCM 13/1/2004.

   Note: Lo IETF RFC 4210 dettaglia alla section 4.4 una procedura utilizzabile per la sostituzione della coppia di chiavi di firma del certificatore.

2. Qualora l'evento indicato all'Art. 25 del DPCM 13/1/2004 si sia già verificato esibisce il relativo verbale.

7.4.3 Il valutatore

1. Verifica l'esistenza della procedura prevista al punto 1 del paragrafo 7.4.2 e che essa corrisponda a quanto indicato nel Piano per la sicurezza.

2. Qualora l'evento indicato all'Art. 25 del DPCM 13/1/2004 si sia già svolto verifica che i verbali della procedura eseguita ne attestino il rispetto.

7.5 Conservazione delle chiavi di certificazione e dei dati per attivarle

Finalità: il certificatore deve assicurare che le chiavi private di certificazione rimangano riservate e conservino la loro integrità.

7.5.1 Normativa

DPCM 13/1/2004

Art. 7. Conservazione delle chiavi.

Art. 33. Organizzazione del personale del certificatore.

Circolare 6 settembre 2005, n. 48

7.5.2 Il certificatore

1. Esibisce procedure operative da cui emerga che esso gestisce i dispositivi di firma in conformità con le Security Policy in base alle quali ai dispositivi stessi è stata riconosciuta la certificazione di sicurezza, in particolare che la chiave privata del certificatore sia custodita in modo sicuro all'interno del relativo dispositivo di firma.

   Nota: per quanto riguarda le copie di sicurezza della chiave privata di firma del certificatore si veda il paragrafo 7.6.

2. Esibisce verbali da cui risulti che le procedure di cui al punto precedente sono state rispettate.

7.5.3 Il valutatore

1. Verifica l'esistenza delle procedure previste al paragrafo 7.5.2 e la loro rispondenza con quanto previsto nella certificazione del dispositivo e con le attribuzioni indicate nella Relazione sulla struttura organizzativa, di cui al punto p) della Circolare CNIPA 48/2005.
2. Verifica che dai verbali di cui al punto 2 del paragrafo 7.5.2 emerga il rispetto delle procedure relative.

Nota: Per le procedure per la esportazione delle chiavi private di certificazione si veda il paragrafo 7.6.

7.6 Copie per backup e recovery delle chiavi di certificazione

Finalità: il certificatore deve assicurare che le chiavi private di certificazione e le loro copie rimangano riservate e conservino la loro integrità.

Nota: le disposizioni in questo paragrafo si applicano ai casi in cui il certificatore preveda la creazione di copie di sicurezza delle proprie chiavi private di firma.

7.6.1 Normativa

DPCM 13/1/2004

Art. 7. Conservazione delle chiavi.

Art. 33. Organizzazione del personale del certificatore.

Art. 34. Requisiti di competenza ed esperienza del personale.

7.6.2 Il certificatore

1. Ove il certificatore esegua copie di sicurezza delle chiavi private di certificazione, esibisce la procedura operativa che deve rispettare i requisiti indicati all'art. 7 comma 2 del DPCM 13/1/2004 e deve essere attuata da personale competente.

   Nota 1: normalmente, laddove i dispositivi di firma utilizzati per i sistemi di CA prevedano l'effettuazione di tali copie di sicurezza, sono previste dal costruttore anche le procedure da eseguire per backup e restore, anch'esse oggetto di valutazione e di certificazione.

   Nota 2: laddove le copie di sicurezza siano protette mediante cifra, la Special Publication 800-57 Part 1 del NIST indica gli anni fino ai quali è probabile resistano algoritmi e lunghezze di chiavi.

2. Ove il certificatore esegua il ripristino delle chiavi private di certificazione, esibisce la procedura operativa che deve rispettare i requisiti indicati all'art. 7 comma 2 del DPCM 13/1/2004 e deve essere attuata da personale competente.
3. Esibisce evidenza che il personale preposto all'esecuzione delle procedure in questione è compreso tra quello indicato agli articoli 33 e 34 del DPCM 13/1/2004, o quanto meno ricade sotto la responsabilità delle figure ivi indicate.
4. In aggiunta alle procedure previste dalle Security Policy dei dispositivi di firma utilizzati per i sistemi di CA, certificati secondo uno dei criteri di sicurezza conformi con quanto previsto all'art. 53 comma 3 del DPCM 13/1/2004, il certificatore esibisce procedure che assicurino che le copie delle chiavi di certificazione o di loro elementi, così come le informazioni atte ad attivarle, siano custodite e accedute secondo modalità che rispettino i requisiti di cui ai commi 2 e 3 dell'art. 7 del DPCM 13/1/2004.
5. Esibisce verbale dell'esecuzione delle procedure di esecuzione delle copie di sicurezza e della loro conservazione.
6. Ove sia stato già effettuato il ripristino delle chiavi di certificazione, il certificatore esibisce il relativo verbale.

7.6.3 Il valutatore

1. Verifica l'esistenza delle procedure previste al paragrafo 7.6.2 e la rispondenza di quella indicata ai punti 1 e 2 del medesimo paragrafo con quanto previsto nella certificazione del dispositivo, ove ivi indicata.
2. Verifica l'esistenza della evidenza che il personale preposto all'esecuzione delle procedure in questione sia compreso tra quello indicato agli articoli 33 e 34 del DPCM 13/1/2004, o che quanto meno ricada sotto la responsabilità delle figure ivi indicate.
3. Verifica la conformità della procedura di cui al punto 4 del paragrafo 7.6.2 con quanto indicato nel Piano per la sicurezza.
4. Verifica che dal verbale previsto al punto n. 5 (ed eventualmente da quello di cui al punto n. 6) del precedente paragrafo 7.6.2 emerga il rispetto di quanto indicato nel Piano per la sicurezza.

7.7 Distribuzione dei certificati delle chiavi di certificazione

Finalità: il certificatore deve assicurare che la autenticità e integrità delle chiavi pubbliche di certificazione siano assicurate durante le fasi della loro distribuzione, dove applicabile.

7.7.1 Normativa

DPCM 13/1/2004

Art. 9. Dispositivi sicuri e procedure per la generazione della firma. – commi 5,6,7

Art. 40. Obblighi per i certificatori accreditati. – commi 1, 3

7.7.2 Il certificatore

1. Qualora preveda la registrazione del certificato del certificatore all'interno del dispositivo sicuro di firma del titolare:
    a. esibisce le registrazioni del giornale di controllo da cui emerga l'attuazione di questa misura;
    b. ove il valutatore lo richieda, gli fornisce dispositivi di firma predisposti per la generazione delle firme.
2. Rende accessibile al valutatore l'ultima versione dell'Elenco Pubblico gestito da CNIPA e da esso pubblicato come da Art. 40 comma 2 del DPCM 13/1/2004.

7.7.3 Il valutatore

1. Può chiedere al certificatore la fornitura di uno o più dispositivi di firma già predisposti per la generazione delle firme
2. Nel caso previsto dal punto 1 del paragrafo 7.7.2:
    a. verifica l'esistenza nel giornale di controllo di registrazioni riconducibili all'inserimento dell'auto-certificato del certificatore all'interno dei dispositivi sicuri di firma dei titolari;

       Nota: la modalità di tenuta del giornale di controllo è verificata al punto 1 del paragrafo 7.1.3;
    b. verifica l'effettiva presenza dell'auto-certificato.
3. Verifica se l'auto-certificato esibito dal certificatore è presente nell'Elenco Pubblico gestito da CNIPA.
4. Verifica se la versione dell'Elenco Pubblico gestito da CNIPA reso accessibile per via telematica dal certificatore presso il proprio sito web sia la più recente, se corrisponda cioè a quella disponibile presso il sito di CNIPA.
5. Verifica nel seguente modo l'autenticità dell'Elenco Pubblico gestito da CNIPA reso accessibile per via telematica dal certificatore presso il proprio sito web:
    a. uno dei certificati rilasciati dal certificatore a CNIPA per la sottoscrizione dell'elenco pubblico dei certificatori, pubblicato nel proprio registro dei certificati, deve corrispondere alla chiave privata con cui è firmato l'Elenco Pubblico gestito da CNIPA;
    b. i digest della chiave pubblica contenuta in tale certificato, calcolati dal valutatore con gli algoritmi pubblicati all'art. 41 comma 5 lettera c) del DPCM 13/1/2004, devono corrispondere a quelli pubblicati più di recente in Gazzetta Ufficiale.

7.8 Key escrow delle chiavi di firma

Finalità: le chiavi private di firma dei titolari non devono essere copiate né conservate da alcuno.

7.8.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere f) e k)

DPCM 13/1/2004

Art. 6. Modalità di generazione delle chiavi. – comma 3

Art. 38. Manuale operativo. – comma 3, lettera h)

7.8.2 Il certificatore

1. Se crea esso stesso le coppie di chiavi di firma dei titolari, esibisce documentazione da cui non risulti che viene trattenuta copia di quella privata.
2. Se è il titolare a creare la coppia di chiavi di firma con una procedura indicata o consegnatagli dal certificatore, quest'ultimo esibisce per tale procedura documentazione che dimostri che la generazione della coppia di chiavi all'interno del dispositivo sicuro di firma rilasciato o indicato dal certificatore sia compatibile con la certificazione di sicurezza del medesimo dispositivo sicuro di firma.

7.8.3 Il valutatore

1. Nel caso previsto dal punto 1 del paragrafo 7.8.2 verifica, salvo quanto previsto al successivo punto 3:
    a. che la descrizione della procedura sia tale da non dare adito a dubbi riguardo il rispetto del requisito di cui all'art. 32 comma 3, punti f) e k), del Dlgs 82/2005;
    b. che l'esecuzione a cura del certificatore della procedura, eseguita in presenza del valutatore, rispecchi quanto in essa descritto.
2. Nel caso previsto dal punto 2 del paragrafo 7.8.2 verifica, salvo quanto previsto al successivo punto 3, che la procedura corrisponda a quanto indicata in tale punto.
3. Qualora il certificatore esibisca verbali di auditing interno o esterno che attestino la rispondenza a cui fanno riferimento i punti precedenti queste verifiche da parte del valutatore possono essere omesse. Il valutatore può verificare l'autenticità di tali verbali.

7.9 Utilizzo della coppia di chiavi di certificazione per ulteriori scopi

Finalità: le chiavi di certificazione possono essere utilizzate solo per gli usi autorizzati.

7.9.1 Normativa

DPCM 13/1/2004

Art. 4. Caratteristiche generali delle chiavi per la creazione e la verifica della firma. – commi 4, lettera b), 5, 6

7.9.2 Il certificatore

1. Esibisce ove del caso l'autorizzazione ricevuta da CNIPA come dal comma 6 dell'art. 4 del DPCM 13/1/2004.

7.9.3 Il valutatore

1. Verifica ove del caso che l'autorizzazione esibita coincida con quella in vigore rilasciata da CNIPA e che gli eventuali altri utilizzi della coppia di chiavi di certificazione non siano anteriori a tale autorizzazione.

2. Può richiedere l'esibizione di certificati emessi in passato secondo le diverse modalità autorizzate da CNIPA.

7.10 Cessazione di una coppia di chiavi di certificazione

Finalità: le chiavi di certificazione non devono essere utilizzate oltre il momento del loro ritiro dall'impiego operativo.

7.10.1 Normativa

La normativa non presenta disposizioni che riguardino esplicitamente come gestire le chiavi di firma del certificatore ritirate dall'attività sia perché il loro certificato è scaduto, sia perché esse sono compromesse direttamente o indirettamente (cioè perché risultano indeboliti l'algoritmo o la loro lunghezza), sia perché il certificatore cessa la propria attività, o per qualsiasi altro motivo. Tuttavia è necessario che al verificarsi di un evento che ne richieda il ritiro dall'impiego operativo tali chiavi siano distrutte così come le loro eventuali copie.

7.10.2 Il certificatore

1. Esibisce una procedura dettagliata (in azioni e rispettivi ruoli) che preveda la distruzione delle chiavi e delle eventuali rispettive copie (totali o parziali) oppure, ove ciò non sia possibile, dei dispositivi che le contengono.

   Tale procedura dovrà essere documentata e basata sulle specifiche di sicurezza secondo le quali il dispositivo è stato certificato.

2. Qualora tale procedura sia stata già eseguita, ne esibisce i verbali.

7.10.3 Il valutatore

1. Verifica che la procedura di cui al punto 1 del paragrafo 7.10.2:
   a. corrisponda a quanto previsto nelle Security Policy di certificazione del dispositivo,
   b. oppure sia sufficientemente dettagliata da spiegare chiaramente come essa abbia per obiettivo il raggiungimento di una distruzione sicura delle chiavi, o di loro porzioni, oppure dei dispositivi che le contengono.
2. Nel caso in cui la procedura di cui al punto 1 del paragrafo 7.10.2 sia stata eseguita, verifica che i verbali di cui al punto 2 del medesimo paragrafo ne attestino il rispetto.

7.11 Gestione del ciclo di vita dei dispositivi di firma del certificatore

Finalità: il certificatore garantisce la sicurezza dei dispositivi di firma per tutto il loro ciclo di vita

7.11.1 Normativa

La normativa non presenta disposizioni che riguardino esplicitamente come gestire i dispositivi di firma del certificatore. Tuttavia è necessario che essi siano gestiti in modo da garantirne la sicurezza.

Nella maggior parte di casi le Security Policy di questi dispositivi prevedono esplicitamente tali misure.

7.11.2 Il certificatore

1. Esibisce procedure dettagliate (in azioni e rispettivi ruoli) che prevedano per questi dispositivi:
    a. i controlli da effettuare alla consegna per accertare che essi non siano stati manomessi durante il trasporto;
    b. le misure da attuare per evitare che essi siano manomessi durante la loro conservazione anteriormente all'attivazione e i controlli relativi;
    c. le operazioni da eseguire, prima di metterli in esercizio, per accertarne il corretto funzionamento;
    d. la loro distruzione all'atto del loro ritiro dall'operatività, oppure la garanzia che il loro contenuto sia definitivamente cancellato in maniera che non ne consenta la ricostruzione;
    e. l'aderenza a quant'altro descritto nel Piano della Sicurezza.

    Tali procedure dovranno essere basate sulle specifiche di sicurezza secondo le quali il dispositivo è stato certificato, ove applicabile.
2. Qualora tali procedure siano state già eseguite, ne esibisce i verbali.

7.11.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui al punto 1 del paragrafo 7.11.2 e verifica che esse
    a. corrispondano a quanto previsto nelle Security Policy di certificazione del dispositivo,
    b. oppure siano sufficientemente dettagliate da spiegare chiaramente come esse portino effettivamente al rispetto dei requisiti indicati al medesimo punto 1 del paragrafo 7.11.2.
2. Nel caso in cui le procedure di cui al punto 1 del paragrafo 7.11.2 siano state eseguite, verifica che i verbali di cui al punto 2 del medesimo paragrafo attestino che la loro effettuazione è stata condotta come previsto.

7.12 Fornitura dei dispositivi sicuri di firma dei titolari da parte del certificatore

Finalità: il certificatore assicura che la generazione da esso effettuata di tutte le coppie di chiavi di firma avvenga in modo sicuro e che garantisca la segretezza della chiave privata.

7.12.1 Normativa

Dlgs 82/2005

Art. 35. Dispositivi sicuri e procedure per la generazione della firma. – commi 1, 2, 4, 5, 6

DPCM 13/1/2004

Art. 5. Generazione delle chiavi. – comma 1

Art. 6. Modalità di generazione delle chiavi. – commi 2, 4

Art. 9. Dispositivi sicuri e procedure per la generazione della firma.

Art. 53. Norme transitorie. – commi 1,2,3

7.12.2 Il certificatore

1. Esibisce, per i dispositivi sicuri di firma che esso distribuisce o il cui uso esso indica ai titolari, documentazione da cui emerga:
    i. la loro rispondenza ai requisiti di sicurezza indicati nella normativa in vigore;
    ii. che i dispositivi predisposti dal certificatore sono custoditi e inoltrati ai titolari in maniera tale da assicurare la segretezza e l'integrità delle chiavi e che, una volta consegnati al titolare, quest'ultimo possa conservare la chiave privata sotto il proprio controllo esclusivo;

    Nota: si veda anche il paragrafo 7.8 Key escrow delle chiavi di firma.
2. Esibisce procedura interna da cui emerga che sono rispettate le misure indicate nella documentazione di valutazione o di certificazione di sicurezza del dispositivo.

7.12.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al punto 1 del paragrafo 7.12.2.
2. Verifica che la documentazione di cui al punto 2 del paragrafo 7.12.2 sia conforme con i requisiti di certificazione.

7.13 Gestione dei dispositivi sicuri di firma dei titolari

Finalità: se il certificatore predispone i dispositivi sicuri di firma dei titolari esso assicura che essi, oltre ad essere conformi con la normativa come da paragrafo 7.12, siano gestiti in sicurezza.

7.13.1 Normativa

A parte la generazione da parte del certificatore delle chiavi di firma, trattata al paragrafo 8.2, e la fornitura dei dispositivi sicuri di firma, trattato al paragrafo 7.12, la normativa non presenta disposizioni che riguardino esplicitamente la predisposizione dei dispositivi sicuri di firma dei titolari da parte del certificatore. Tuttavia è necessario che essi siano gestiti in modo da garantirne la sicurezza.

Nella maggior parte dei casi le Security Policy di questi dispositivi prevedono esplicitamente tali misure.

7.13.2 Il certificatore

1. In aggiunta a quanto indicato ai paragrafi 8.2 e 7.12, esibisce procedure dettagliate (in azioni e rispettivi ruoli) per la preparazione di questi dispositivi che prevedano:
    a. la tenuta di un inventario a cura di uno dei Responsabili indicati dal DPCM 13/1/2004, art. 33.
    b. la loro conservazione e distribuzione in modo sicuro;
    c. la distribuzione, ove applicabile, dei dati per la loro attivazione (ad esempio il PIN) effettuata in modo sicuro, ad esempio se dispositivo e dati per l'attivazione sono spediti al titolare e non sono consegnati personalmente, la spedizione dei due oggetti deve avvenire in modo separato.

    Tali procedure, ove applicabile, dovranno essere basate sulle security policy secondo le quali il dispositivo è stato certificato.
2. Qualora si sia già verificata l'esecuzione di tali procedure, esibisce documentazione che ne comprovi il rispetto.

7.13.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui al punto 1 del paragrafo 7.13.2 e verifica che esse
    a. corrispondano, ove applicabile, a quanto previsto nelle Security Policy di certificazione dei dispositivi,
    b. oppure siano sufficientemente dettagliate da illustrare chiaramente il rispetto dei requisiti indicati al medesimo punto 1 del paragrafo 7.13.2.
2. Nel caso in cui le procedure di cui al punto 1 del paragrafo 7.13.2 siano state eseguite, verifica che i documenti di cui al punto 2 del medesimo paragrafo vi corrispondano.

Capitolo 8

Servizi di gestione dei certificati

8.1 Servizio di Registrazione dei titolari

Finalità: il certificatore verifica in modo affidabile l'identità dei titolari e, ove richiesto, il loro diritto ad avere rappresentati nel proprio certificato eventuali titoli o ruoli specifici, ivi inclusi eventuali limiti alle negoziazioni. I risultati di questo servizio sono inoltrati al "Servizio di generazione dei certificati".

8.1.1 Normativa

Dlgs 82/2005

Art. 23. Copie di atti e documenti informatici. – commi 2-bis, 3, 4, 5, 7

Art. 28. Certificati qualificati. – commi 2, 3

Art. 30. Responsabilità del certificatore. – commi 1 lettera a), 3

Art. 32. Obblighi del titolare e del certificatore. – commi 1, 3, lettere a), c), e), j), l), m), 4, 5

Art. 33. Uso di pseudonimi.

DPCM 13/1/2004

Art. 7. Conservazione delle chiavi. – commi 1, 3

Art. 9. Dispositivi sicuri e procedure per la generazione della firma. – commi 3, lettera a), 7

Art. 15. Informazioni contenute nei certificati qualificati. – comma 3

Nota: con l'entrata in vigore del Dlgs 159/2006 il termine di conservazione delle informazioni di cui a questo articolo è stato portato a venti anni.

Art. 26. Revoca dei certificati relativi a chiavi di certificazione. – comma 2

Art. 38. Manuale operativo. – comma 3 lettera g)

Art. 43. Limitazioni d'uso.

Del CNIPA 4/2005

Art. 4. Profilo dei certificati qualificati – commi 1, 2, 3, 4, 5, lettera f), punto 2

8.1.2 Il certificatore

1. Esibisce procedure operative dettagliate, e relativa documentazione (quali verbali, dichiarazioni del richiedente, ecc.), che dimostrino che in fase di registrazione il certificatore, o chi da esso delegato, in modo affidabile e in conformità con quanto indicato nel Manuale operativo:
    a. verifica l'identità del titolare;
    b. associa al titolare i dati identificativi del dispositivo sicuro di firma;
    c. verifica il diritto, ove del caso, del titolare a far indicare nel certificato:
        i. "*qualifiche specifiche*";
        ii. "*poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite*";
        iii. "*limiti d'uso del certificato*";
        iv. *"limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili"*;

        e verifica, ove del caso, il relativo consenso del terzo interessato;
    d. associa al titolare il certificato ad esso attribuito, anche ove in esso sia indicato uno pseudonimo.
2. Esibisce i test set, e i relativi verbali di corretta esecuzione dei medesimi, da cui emerga che i dati immessi vengono adeguatamente controllati prima di essere inseriti nel certificato del titolare.

    Nota: tale controllo può essere effettuato a posteriori sul certificato emesso, anche se questo comporta un inutile appesantimento delle CRL.
3. Ove la registrazione dei titolari sia subordinata a un preventivo accordo con un'organizzazione, il certificatore esibisce documentazione, ivi inclusi eventuali verbali di audit, da cui emerga che:
    a. in sede di stipula di tale accordo, esso verifica:
        i. l'effettiva esistenza dell'organizzazione con cui l'accordo viene stipulato;
        ii. il diritto da parte di chi sottoscrive l'accordo a rappresentare l'organizzazione nella stipula dell'accordo.
    b. in sede di registrazione del richiedente, esso verifica l'appartenenza del medesimo all'organizzazione interessata.
4. Esibisce documentazione (ad esempio verbali, dichiarazioni dei richiedenti, ecc.) e procedure operative che dimostrino che esso:
    a. informa tempestivamente "*i richiedenti* [dei certificati] *in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione*"; in particolare che il titolare:
        i. deve inoltrare la richiesta di certificazione e di sospensione o revoca del certificato con le modalità indicate nel Manuale operativo;
        ii. qualora la firma digitale sia apposta per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso (DPCM 13/1/2004 art. 4 comma 2) e rendere palese la sua adozione in relazione al singolo documento firmato automaticamente (Dlgs 82/2005 art. 35 comma 3);
        iii. non deve duplicare la chiave privata né il dispositivo sicuro di firma che la contiene;
        iv. non deve utilizzare la chiave di firma per funzioni diverse da quelle previste nel certificato;

v. deve utilizzare algoritmi di firma e coppie di chiavi conformi con quanto indicato nel DPCM in vigore che riporta le regole tecniche;

vi. perché le firme digitali abbiano valore legale, deve apporle esclusivamente a documenti privi di macroistruzioni e codice atti a modificare atti, dati e fatti rappresentati nel documento;

vii. deve utilizzare esclusivamente i formati di firma previsti dalla normativa;

viii. deve conservare con la massima diligenza la chiave privata e il dispositivo sicuro di firma che la contiene al fine di garantirne l'integrità e la massima riservatezza;

ix. deve conservare con la massima diligenza e separatamente dal dispositivo sicuro di firma, al fine di garantirne la massima riservatezza, i codici di abilitazione all'uso della chiave privata, i codici per richiedere la sospensione in emergenza ed eventuali altri codici riservati;

x. deve richiedere immediatamente la revoca dei certificati relativi alle chiavi contenute in dispositivi sicuri di firma di cui abbia perduto il possesso o il controllo esclusivo o che siano difettosi;

xi. non deve apporre firme digitali avvalendosi di chiavi private delle quali sia stato revocato il certificato (Dlgs 82/2005, art. 24 comma 3);

xii. non deve apporre firme digitali avvalendosi di chiavi private il cui certificato sia stato emesso in base a un certificato di certificazione che a lui sia noto essere stato revocato;

xiii. chiedere tempestivamente la revoca del proprio certificato in caso si siano modificate, o siano venute meno, le circostanze oggetto delle informazioni rappresentate nel certificato stesso (Dlgs 82/2005); questo è tanto più vero laddove l'utilizzo di un certificato errato o con informazioni obsolete possa provocare danni ad altri (Dlgs art. 28 comma 4 e art. 32 comma 1);

xiv. deve redigere e sottoscrivere la richiesta di revoca dei propri certificati, specificandone decorrenza e motivazione, e presentarla secondo le modalità indicate nel Manuale Operativo;

xv. deve presentare la richiesta di sospensione, indicandone la durata, seguendo le modalità indicate nel Manuale Operativo;

xvi. deve svolgere le azioni previste dal certificatore per il caso di smarrimento o sottrazione del dispositivo sicuro di firma, opportunamente evidenziate nella informativa rilasciata dal certficatore stesso;

xvii. deve adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;

xviii. deve utilizzare personalmente il dispositivo sicuro di firma.

Nota: una tale informativa può anche essere ottenuta mediante altri sistemi, come ad esempio pubblicazione dei termini e delle condizioni sul sito del certificatore, purché i richiedenti la certificazione siano chiaramente invitati ad accedere a tale sito.

b. informa tempestivamente i terzi interessati dei loro obblighi, tra cui i seguenti:

i. richiedere la revoca di un certificato ogniqualvolta vengano meno i requisiti in base ai quali esso è stato rilasciato al Titolare;

ii. sottoscrivere la richiesta di revoca o sospensione, indicando anche la motivazione nel primo caso e la durata nel secondo caso, e presentarla al Certificatore come indicato nel Manuale Operativo;

iii. porre i Titolari che a lui afferiscono a conoscenza delle tematiche di sicurezza concernenti l'uso della firma digitale: custodia del dispositivo sicuro di firma, accesso ai sistemi, ecc.;

iv. rispettare eventuali ulteriori obblighi indicati nello specifico accordo tra l'organizzazione di appartenenza del Terzo interessato e il Certificatore;

c. predispone "*su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione*";

d. *"raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196"* ;

e. utilizza per altri scopi i dati personali raccolti ai fini delle attività di certificazione, solo dopo aver ricevuto "*l'espresso consenso della persona cui si riferiscono*";

f. acquisisce *"per i titolari residenti all'estero cui non risulti attribuito il codice fiscale,… il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale*";

g. conserva "*le informazioni relative alla reale identità del titolare per almeno* [venti] *anni dopo la scadenza del certificato stesso*";

h. è organizzato in modo da *"tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari*";

i. rende i certificati "*accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato*", il che può essere realizzato, in alternativa:

   i. richiedendo esplicito consenso a tale pubblicazione e pubblicando solo i certificati per i quali esso sia stato ottenuto, tenendo conto di eventuali limitazioni espresse dal titolare;

   ii. non richiedendo alcun consenso di questo tipo e non pubblicando mai i certificati.

   Nota: La assenza di pubblicazione dei certificati non crea alcun ostacolo alla verifica delle firme elettroniche mentre aggiunge sicurezza al sistema, stante il dettato dell'art. 36 del DPCM 13/1/2004 ("*Alla firma digitale deve essere allegato il certificato qualificato corrispondente alla chiave pubblica da utilizzare per la verifica.*").

5. Qualora si avvalga di servizi di registrazione effettuati da una terza parte, esibisce gli accordi che impegnano quest'ultima a seguire procedure analoghe a quelle indicate ai punti precedenti e a redigere documentazione analoga a quella richiesta al precedente punto1.

   Nota: il dettato dell'art. 30 comma 1 del Dlgs 82/2005, sopra citato, attribuisce al certificatore la responsabilità di erronee e incomplete informazioni riportate nel certificato. La lettera a) di tale articolo 30 comma 1 non si applica solo alla rappresentazione all'interno del certificato stesso della chiave pubblica e alla firma del certificatore, ma anche a tutte le altre informazioni ivi riportate.

6. Esibisce documentazione atta a provare che i dati di registrazione dei titolari sono tenuti in modo conforme a quanto previsto nel Dlgs 196/2003 per i dati personali.

8.1.3 Il valutatore

1. Verifica l'esistenza delle procedure e della documentazione di cui al paragrafo 8.1.2 e che in esse sia prevista l'attuazione delle misure ivi indicate.
2. Nel caso in cui le procedure di cui al paragrafo 8.1.2 siano già state eseguite, verifica che i verbali e gli analoghi documenti di cui allo stesso paragrafo attestino il rispetto delle medesime procedure e, ove invece sia stato riscontrato il mancato rispetto delle procedure, che siano state intraprese dal certificatore le opportune azioni correttive.
3. Verifica, ove del caso, l'esistenza degli accordi previsti al punto 5 del paragrafo 8.1.2.
4. Può effettuare verifiche presso le terze parti incaricate di fornire il servizio di registrazione onde verificare il rispetto di quanto previsto al paragrafo 8.1.2.

8.2 Generazione delle coppie di chiavi di sottoscrizione

Finalità: il certificatore assicura che la chiave pubblica inclusa in una richiesta di certificazione, a fronte della quale il "Servizio di generazione dei certificati" successivamente genererà un certificato, corrisponda a una chiave privata custodita all'interno del dispositivo sicuro di firma del titolare e che, se generata da quest'ultimo, sia stata generata all'interno del dispositivo stesso.

8.2.1 Normativa

DPCM 13/1/2004

Art. 6. Modalità di generazione delle chiavi. – commi 3, 5

Art. 8. Generazione delle chiavi al di fuori del dispositivo di firma.

Art. 38. Manuale operativo. – comma 3, lettera h)

Art. 53. Norme transitorie. – comma 3

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

d) garanzie relative al sistema di generazione delle chiavi;

e) caratteristiche del sistema di generazione;

[omissis]

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

8.2.2 Il certificatore

1. Esibisce procedure operative, conformi con quanto da esso stesso indicato nella dichiarazione tecnica richiesta dalla Circolare CNIPA 48/2005, che dimostrino che:
    a. se la coppia di chiavi è generata dal certificatore al di fuori del dispositivo sicuro di firma il trasferimento, almeno per quanto riguarda la chiave privata, all'interno del dispositivo sicuro di firma avviene in modo sicuro;
    b. se la coppia di chiavi è generata dal titolare, la sua generazione avviene all'interno del dispositivo sicuro di firma.
    c. in alternativa, la coppia di chiavi sia generata dal certificatore all'interno del dispositivo sicuro di firma.
2. Esibisce procedure operative e certificazioni di sicurezza che dimostrino che si utilizzano esclusivamente dispositivi sicuri di firma conformi con quanto previsto all'art. 53 comma 3 del DPCM 13/1/2004 o sue successive modificazioni e integrazioni
3. Esibisce documentazione che confermi il rispetto delle procedure di cui ai punti 1 e 2.

8.2.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui ai punti 1 e 2 del paragrafo 8.2.2 e che in esse sia prevista l'attuazione delle misure ivi indicate.
2. Verifica che la documentazione di cui al punto 3 del paragrafo 8.2.2 dimostri il rispetto delle procedure di cui ai punti 1 e 2 del medesimo paragrafo.

8.3 Servizio di generazione dei certificati qualificati

Finalità: il certificatore genera in modo sicuro e sottoscrive certificati basati sull'identità e sugli attributi del titolare verificati in fase di registrazione, assicurando che la chiave pubblica inclusa nel certificato corrisponda a una chiave privata della quale il titolare abbia il controllo esclusivo.

8.3.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettere d), e)

Art. 32. Obblighi del titolare e del certificatore. – commi 2, 3, lettera i)

DPCM 13/1/2004

Art. 9. Dispositivi sicuri e procedure per la generazione della firma. – commi 1, 2, 3

Art. 14. Generazione dei certificati qualificati.

Art. 15. Informazioni contenute nei certificati qualificati. – commi 1, lettera a), 3, 4

Art. 27. Requisiti di sicurezza dei sistemi operativi.

Art. 28. Sistema di generazione dei certificati qualificati.

Art. 30. Piano per la sicurezza. – comma 1, lettera g)

Nota: ovviamente l'intero Piano per la sicurezza afferisce il Servizio di generazione dei certificati, anche se qui viene enfatizzata solo la descrizione delle procedure utilizzate.

Art. 37. Codice di emergenza. – commi 1, 3

Art. 39. Riferimenti temporali opponibili ai terzi. – commi 1, 2, 3

Art. 38. Manuale operativo. – comma 3, lettera i)

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

l) caratteristiche del sistema di generazione dei certificati;

8.3.2 Il certificatore

1. Esibisce documentazione comprovante la rispondenza dei dispositivi di firma e dei sistemi operativi da esso utilizzati ai requisiti di certificazione previsti agli articoli 9 comma 3 e 27 del DPCM 13/1/2004.
2. Esibisce procedure operative conformi con quanto descritto nel proprio Piano per la Sicurezza, previsto dall'art. 30 del DPCM 13/1/2004, volte ad assicurare l'affidabilità dei sistemi e dei prodotti di firma, nonché l'adozione di misure contro la contraffazione dei certificati, di cui all'art. 27 del Dlgs 82/2005 e agli artt. 9 e 28 del DPCM 13/1/2004.
3. Per quanto riguarda l'attestazione del momento di emissione dei certificati in modo conforme al requisito indicato all'art. 14 comma 4 del DPCM 13/1/2004, fornisce evidenza del corretto funzionamento delle procedure che garantiscono la conformità del riferimento temporale registrato sul giornale di controllo con quanto indicato all'art. 39 comma 3 del DPCM 13/1/2004.
4. Nel caso di richieste di certificazione sottoposte dal titolare esibisce procedure atte a dimostrare come precedentemente all'emissione dei certificati vengano verificati l'autenticità della relativa richiesta e il possesso della corrispondente chiave privata da parte del titolare.

5. Nel caso di richieste di certificazione prodotte direttamente dal certificatore esibisce procedure atte a dimostrare che il certificato prodotto e la corrispondente chiave privata, custodita all'interno del dispositivo sicuro di firma, siano consegnati al titolare in maniera sicura, tale, cioè, da non compromettere la riservatezza della chiave privata e il suo uso esclusivo da parte del titolare.
6. Esibisce procedure che dimostrino come il codice identificativo del titolare riportato nel certificato, come richiesto dall'art. 15 comma 1 del DPCM 13/1/2004, sia univocamente collegato al titolare.
7. Esibisce documentazione atta a comprovare l'adozione di algoritmi e chiavi di lunghezza conformi con le norme vigenti in materia. Per quanto concerne la scelta della lunghezza delle chiavi crittografiche di cui all'art. 53 comma 1 del DPCM 13/1/2004, il certificatore esibisce, a supporto della scelta effettuata, documentazione tecnica generalmente riconosciuta, quale il documento NIST SP800-57-1 o lo ETSI TS 102 176-1.
8. Esibisce procedure operative e tecniche comprovanti l'attribuzione a ogni titolare di un codice riservato da utilizzare nelle richieste in emergenza di sospensione o revoca del proprio certificato e la sicurezza e la riservatezza nell'uso del medesimo.
9. Ove richiesto dal valutatore, genera appositamente certificati atti a consentire al valutatore stesso le verifiche di cui in questo paragrafo, come anche la verifica che i dati del certificato non diano adito ad equivoci sull'identità del certificatore.
10. Ove richiesto dal valutatore può alterare l'ora del sistema di generazione dei certificati, in ambiente di test, onde consentire il riscontro delle azioni correttive.
11. Esibisce i verbali comprovanti la regolare effettuazione delle procedure suddette.

8.3.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui al paragrafo 8.3.2 e che in esse sia prevista l'attuazione delle misure ivi indicate. In particolare si raccomanda di verificare che esse esplicitamente prevedano che la richiesta di certificazione soddisfi tutti i seguenti requisiti:
    a. ove non generata direttamente dal certificatore, gli pervenga in modo da assicurare che essa sia stata generata dal titolare o, sotto la sua diretta supervisione, da specifici addetti incaricati dal certificatore, e che sia tale da assicurare che la corrispondente chiave privata sia stata generata e sia custodita all'interno di un dispositivo sicuro di firma attribuito o indicato dal certificatore;
    b. ove sia generata dal certificatore, assicuri la riservatezza della chiave privata e il suo uso esclusivo da parte del titolare e che la consegna a quest'ultimo del certificato e del dispositivo sicuro di firma contenente la chiave privata avvenga con modalità sicure;
    c. i dati identificativi del titolare contenuti nella richiesta di certificazione corrispondano ai dati del titolare acquisiti in modo sicuro all'atto della sua registrazione da parte degli addetti a tale mansione e da questi ultimi inoltrati in maniera sicura al certificatore, e quindi custoditi in modo sicuro, tale cioè da non consentirne una modifica non autorizzata.
2. Verifica l'esistenza e correttezza dei verbali di cui al paragrafo 8.3.2.
3. Può chiedere la generazione di certificati atti a consentire al valutatore stesso le verifiche di cui in questo paragrafo, come anche la verifica che i dati del certificato non diano adito ad equivoci sull'identità del certificatore
4. Può chiedere l'alterazione dell'ora del sistema di generazione dei certificati, in ambiente di test, onde riscontrare le azioni correttive.
5. Verifica che i dati riportati nel certificato non possano creare equivoci sull'identità del certificatore.

8.4 Formato e contenuto dei certificati qualificati

Finalità: il certificatore genera certificati basati sull'identità (o pseudonimo) e sugli eventuali titoli, ruoli e quant'altro verificato in fase di registrazione associandoli a una chiave pubblica la cui corrispondente chiave privata sia in possesso del titolare. Questi certificati sono emessi nel rispetto dei requisiti indicati nella normativa allo scopo di garantire l'interoperabilità tra i certificati emessi dai vari certificatori.

8.4.1 Normativa

Dlgs 82/2005

Art. 24. Firma digitale – comma 4

Art. 28. Certificati qualificati. – commi 1, 2, 3

Art. 30. Responsabilità del certificatore. – commi 1, lettere a), b), c), 3

Art. 33. Uso di pseudonimi.

DPCM 13/1/2004

Art. 3. Norme generali

Art. 4. Profilo dei certificati qualificati – comma 1

Art. 15. Informazioni contenute nei certificati qualificati. – commi 1, 2, 3

Art. 35. Formato dei certificati qualificati.

Art. 38. Manuale operativo. – comma 3, lettere i), l)

Nota: la Deliberazione CNIPA 4/2005 impone all'art. 4.5 lettera f) che l'indicazione che il certificato è un certificato qualificato sia fornita mediante l'uso della certificate extension qcStatements definita nello ETSI TS 101 862

Art. 43. Limitazioni d'uso.

Deliberazione CNIPA 4/2005

Titolo II – PROFILO DEI CERTIFICATI QUALIFICATI

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

f) informazioni contenute nei certificati;

8.4.2 Il certificatore

1. Dietro richiesta del valutatore, volta a verificare il rispetto dei requisiti indicati agli articoli 28 e 30 comma 3 del Dlgs 82/2005, agli artt. 15 e 43 del DPCM 13/1/2004, al Titolo II della Deliberazione CNIPA N. 4/2005 e dichiarati dal certificatore ai sensi della Circolare CNIPA 48/2005, in particolare che i certificati riportino i dati indicati nei citati dispositivi giuridici:
    a. esibisce alcuni certificati qualificati da esso generati,
    b. ne emette alcuni di prova che provvederà a sospendere e a revocare su richiesta del valutatore e comunque dopo il termine dell'ispezione.
2. Esibisce la documentazione riferita ai titolari comprovante la veridicità dei dati riportati nei certificati qualificati.

3. Esibisce procedure atte a dimostrare che la chiave pubblica inclusa nei certificati corrisponde alla chiave privata in effettivo possesso del titolare.
4. Ove siano stati emessi certificati riferiti a pseudonimi, esibisce la documentazione corrispondente prevista all'art. 33 del Dlgs 82/2005.
5. Qualora il campo authorityKeyIdentifier contenga un valore keyIdentifier non calcolato conformemente con quanto raccomandato dalla specifica pubblica IETF RFC 3280 il certificatore esibisce documentazione che fornisca adeguata motivazione per aver deviato da tale indicazione.

   Nota: come richiesto nello RFC 3280 il valore keyIdentifier DOVREBBE (SHOULD) essere ottenuto dalla rispettiva chiave pubblica tramite algoritmo di hashing SHA-1 oppure tramite un sistema che assicuri valori unici.

8.4.3 Il valutatore

1. Richiede l'esibizione di alcuni certificati qualificati emessi per alcuni titolari onde verificare il rispetto dei requisiti indicati agli articoli 28 e 30 comma 3 del Dlgs 82/2005 e 15 e 43 del DPCM 13/1/2004, in particolare che i certificati riportino i dati indicati nei citati dispositivi giuridici.
2. Può chiedere l'emissione di certificati di prova. Di questi certificati può chiedere la sospensione e la revoca come indicato al successivo capitolo 8.10.3. Il certificatore è tenuto a revocare comunque tali certificati dopo il termine dell'ispezione qualora essi non siano già stati revocati durante l'ispezione stessa.
3. Verifica che i certificati qualificati rispettino quanto indicato nel Titolo II della Deliberazione CNIPA N. 4/2005 e quanto dichiarato dal certificatore nella dichiarazione tecnica fornita al CNIPA come da Circolare CNIPA 48/2005.
4. Verifica l'esistenza della documentazione di cui al paragrafo 8.4.2.
5. Verifica l'esistenza di procedure atte a dimostrare che la chiave pubblica inclusa nei certificati corrisponda alla chiave privata in effettivo possesso del titolare, provvedendo, ove del caso, ad effettuare verifiche di firme emesse con tali chiavi private.

8.5 Algoritmi

Finalità: gli algoritmi che il certificatore utilizza direttamente e quelli su cui si basano i dispositivi sicuri di firma che esso consegna o indica ai titolari, così come i programmi di verifica che esso fornisce ai propri titolari, devono essere conformi alla normativa; esso inoltre deve indicare ai propri titolari quali algoritmi e quali lunghezze minime di chiavi essi devono utilizzare nelle loro applicazioni di firma. Qualora il certificatore fornisca ai titolari anche un programma per l'apposizione delle firme tale programma deve avvalersi dei medesimi algoritmi e di analoghe coppie di chiavi.

8.5.1 Normativa

DPCM 13/1/2004

Art. 3. Norme tecniche di riferimento. – commi 1, 2

Art. 5. Generazione delle chiavi.

Art. 10. Verifica delle firme digitali.

Art. 30. Piano per la sicurezza. – comma 1, lettera f)

Art. 53. Norme transitorie. – commi 1, 2

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

a) algoritmi di generazione e di verifica delle firme utilizzati e supportati dal certificatore;

b) algoritmi di hash utilizzati e supportati dal certificatore;

c) lunghezza delle chiavi;

8.5.2 Il certificatore

1. Esibisce documentazione che dimostri:
   a. l'adozione degli algoritmi e delle chiavi, conformi con quanto previsto nel DPCM 13/1/2004, da esso stesso indicati nel Piano per la sicurezza di cui all'art. 30 del medesimo DPCM e/o nella dichiarazione tecnica richiesta dalla Circolare CNIPA 48/2005;
   b. adeguata informativa fornita ai titolari sull'obbligo da parte loro di utilizzare applicazioni di firma che si avvalgano di algoritmi analogamente conformi;
   c. la fornitura ai titolari di applicazioni di verifica delle firme in grado di gestire gli algoritmi suddetti.

   Nota: di questa documentazione fa parte la certificazione dei dispositivi di firma propri e di quelli indicati o consegnati ai titolari, integrata dalle procedure di generazione delle chiavi e delle firme in vigore presso il certificatore e consegnate ai titolari con l'obbligo di avvalersene.

8.5.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al punto 1 del paragrafo 8.5.2.

8.6 Termini e condizioni

Finalità: il certificatore assicura di fornire una tempestiva, duratura e comprensibile informazione al titolare sui termini e sulle condizioni contrattuali.

8.6.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera l)

8.6.2 Il certificatore

1. Esibisce procedure operative che dimostrino che esso informa con tempestività, chiaramente e compiutamente coloro che richiedono il suo servizio di certificazione, sui termini e sulle condizioni relative al servizio da esso fornito avvalendosi di mezzi durevoli.

   Nota: ulteriori approfondimenti su questo argomento si possono trovare al paragrafo 8.1.

8.6.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui al punto 1 del precedente paragrafo 8.6.2.

8.7 Rinnovo della coppia di chiavi, dei certificati, aggiornamento di questi ultimi

Finalità: assicurare che le richieste di rinnovo di certificati a seguito di rinnovo di coppie di chiavi, o di variazioni dei dati riportati nei certificati, avvengano in sicurezza.

Nota: questo caso non riguarda la sostituzione di un certificato già scaduto o revocato nei quali casi sarà necessario seguire una procedura che fornisca almeno le stesse garanzie di sicurezza della procedura di rilascio.

8.7.1 Normativa

Non esistono disposizioni normative relative specificamente a questo caso, ma ad esso si applica quanto afferisce la iniziale richiesta ed emissione dei certificati.

Si applica quanto già citato al paragrafo 8.3 relativamente agli articoli dei dispositivi seguenti:

Dlgs 82/2005

Art. 27. Certificatori qualificati.

Art. 32. Obblighi del titolare e del certificatore.

DPCM 13/1/2004

Art. 9. Dispositivi sicuri e procedure per la generazione della firma.

Art. 14. Generazione dei certificati qualificati.

Art. 15. Informazioni contenute nei certificati qualificati.

Art. 27. Requisiti di sicurezza dei sistemi operativi.

Art. 28. Sistema di generazione dei certificati qualificati.

Art. 30. Piano per la sicurezza.

Art. 35. Formato dei certificati qualificati.

Art. 37. Codice di emergenza.

Art. 38. Manuale operativo.

Art. 39. Riferimenti temporali opponibili ai terzi.

8.7.2 Il certificatore

1. Esibisce procedure operative che dimostrino che, in aggiunta alle misure indicate al paragrafo 8.3.2, esso:
    a. verifica che, qualora l'autenticità della richiesta di un nuovo certificato sia garantita da uno precedente, quest'ultimo non sia scaduto né revocato; in caso contrario il richiedente dovrà seguire le medesime procedure utilizzate all'atto della prima registrazione o altre che forniscano garanzie di sicurezza almeno ad esse equivalenti;
    b. assicuri che al richiedente siano note le versioni più aggiornate dei termini e condizioni contrattuali;
    c. qualora sia richiesta l'emissione di un nuovo certificato a fronte di una pre-esistente coppia di chiavi, emette il nuovo certificato soltanto se la robustezza di questa coppia di chiavi sia adeguata al periodo previsto di validità del certificato da emettere, analogamente a quanto indicato al punto 7 del paragrafo 8.3.2.
2. Dietro richiesta del valutatore, ove del caso, esegue la procedura di rinnovo di un certificato revocato o scaduto per dimostrare che esso non può essere rinnovato.

8.7.3 Il valutatore

1. Verifica l'esistenza delle procedure di cui al paragrafo 8.3.2 relativo al Servizio di generazione dei certificati qualificati e del paragrafo 8.7.2, e che in esse sia prevista l'attuazione delle misure ivi indicate.
2. Può, ove del caso, richiedere il rinnovo di un certificato da lui ottenuto per l'effettuazione delle attività di vigilanza e che sia revocato o scaduto, onde verificare che tale rinnovo non sia effettuato.

8.8 Formato dei certificati di marcatura temporale

Finalità: assicurare il rispetto dei requisiti indicati nella normativa, allo scopo di conservare l'interoperabilità tra i certificati di marcatura temporale emessi dai vari certificatori.

8.8.1 Normativa

DPCM 13/1/2004

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 3

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

g) formato dei certificati;

8.8.2 Il certificatore

1. Esibisce i certificati dei sistemi di marcatura temporale, nell'ambito delle possibilità offerte dalle combinazioni previste dalla Deliberazione CNIPA 4/2005 e da esso realizzate come indicato nel Manuale Operativo, da cui emerga il rispetto dei requisiti giuridici.

8.8.3 Il valutatore

1. Verifica che i certificati di marcatura temporale emessi dal certificatore siano conformi con i requisiti della Deliberazione CNIPA 4/2005 e con quanto indicato nel Manuale Operativo del certificatore.

8.9 Servizio divulgativo

Finalità: Rendere disponibile i certificati al titolare ed, eventualmente, alle terze parti interessate e, nei casi consentiti dal titolare del certificato, ad altri soggetti.

8.9.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera m)

DPCM 13/1/2004

Art. 29. Accesso del pubblico ai certificati. – commi 1, 2

Art. 27. Requisiti di sicurezza dei sistemi operativi. – comma 1

Art. 38. Manuale operativo. – commi 1, 3, lettere o), p)

Art. 40. Obblighi per i certificatori accreditati. – commi 1, 2, 3

8.9.2 Il certificatore

1. Esibisce documentazione e procedure operative che dimostrino che:
    a. il registro di certificati opera su un sistema il cui sistema operativo è conforme almeno con ITSEC F C2/E2;
    b. l'accesso al registro dei certificati è controllato in modo che soltanto le persone autorizzate possano effettuare inserimenti e modifiche;
    c. l'autenticità delle informazioni contenute nel registro dei certificati è verificabile;
    d. l'operatore può rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza del registro dei certificati;
    e. le modalità di gestione del registro dei certificati e quelle di accesso ad esso sono conformi con quanto dichiarato nella documentazione consegnata ai sensi della Circolare CNIPA 48/2005;
    f. i certificati, se pubblicati nel registro dei certificati, sono accessibili alla consultazione del pubblico soltanto nei casi consentiti dai titolari e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.
2. Esibisce prova che per ciascuna delle chiavi di firma elettronica utilizzate dal CNIPA per la sottoscrizione dell'elenco pubblico dei certificatori abbia emesso un certificato qualificato e che tali certificati siano pubblicati nel proprio registro dei certificati.

8.9.3 Il valutatore

1. Verifica l'esistenza dei documenti e delle procedure di cui al paragrafo 8.9.2.
2. Verifica che nel registro dei certificati non esistano certificati, ai quali sia possibile accedere liberamente, per i quali non sia esibita autorizzazione da parte del titolare a tale accesso generalizzato.
3. Può chiedere l'emissione di certificati di prova per i quali non dia l'autorizzazione all'accesso indiscriminato, onde verificarne l'effettiva impossibilità di accedervi.
4. Verifica che il periodo di tempo utile per accedere al contenuto del registro dei certificati, ivi incluse le informazioni sullo stato dei certificati (vedere Capitolo 8.10), sia conforme con la disponibilità indicata nel Manuale operativo.

8.10 Servizio di gestione delle revoche

Finalità: Elaborare tempestivamente, previa adeguata autenticazione del richiedente, le richieste relative alle revoche o sospensioni di certificati, per determinare le azioni da intraprendere. I risultati di questo servizio sono distribuiti attraverso il "Servizio di informazione sullo stato dei certificati" .

8.10.1 Normativa

Dlgs 82/2005

Art. 21. Valore probatorio del documento informatico sottoscritto. – comma 3

Art. 28. Certificati qualificati. – comma 4

Art. 30. Responsabilità del certificatore. – comma 2

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere h), i), j)

Art. 36. Revoca e sospensione dei certificati qualificati.

DPCM 13/1/2004

Art. 16. Revoca e sospensione del certificato qualificato.

Art. 17. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione.

Art. 18. Revoca su iniziativa del certificatore.

Art. 19. Revoca su richiesta del titolare.

Art. 20. Revoca su richiesta del terzo interessato.

Art. 21. Sospensione dei certificati qualificati.

Art. 22. Sospensione su iniziativa del certificatore.

Art. 23. Sospensione su richiesta del titolare.

Art. 24. Sospensione su richiesta del terzo interessato.

Art. 26. Revoca dei certificati relativi a chiavi di certificazione. – comma 3

Art. 37. Codice di emergenza.

Art. 38. Manuale operativo. – commi 1, 2, 3, lettera m)

Art. 46. Chiavi di marcatura temporale. – comma 2

8.10.2 Il certificatore

1. Esibisce documentazione, ivi inclusi i log, e procedure operative che dimostrino che:
    a. le richieste di sospensione e di revoca vengono elaborate non appena ricevute entro l'orario di servizio indicato nel Manuale operativo;
    b. le richieste di sospensione e revoca sono conservate per il periodo previsto dalla normativa, come tutte le informazioni relative al certificato, in conformità con quanto previsto dall'art. 32 comma 3 lettera j del Dlgs 82/2005;
    c. prima di elaborare una richiesta di sospensione e di revoca viene verificato, secondo quanto indicato nel Manuale operativo, che essa provenga effettivamente da una persona autorizzata: titolare, terzo interessato, autorità competente, il certificatore stesso;
    d. qualora non sia possibile completare tempestivamente la verifica dell'autenticità della richiesta il certificato viene sospeso per il periodo necessario ad effettuare tale verifica;

        Nota 1: per "tempestivamente" si intende in tempo utile per la pubblicazione dell'eventuale revoca nella CRL immediatamente successiva;

        Nota 2: la durata di questa sospensione DOVREBBE essere limitata a un valore massimo prefissato e noto onde limitare possibili attacchi di Denial of Service.

    e. esiste un sistema, basato su un codice la cui segretezza deve essere assicurata dal certificatore, che consente la sospensione in emergenza del certificato; a tale richiesta di sospensione deve seguire una conferma debitamente sottoscritta per potere procedere alla revoca;

        Nota 3: il sistema di autenticazione della richiesta di sospensione deve tenere conto della possibilità che, successivamente, la sospensione possa essere ritirata, e che quindi il codice di emergenza possa essere riutilizzato. Analoga soluzione deve essere impiegata laddove si abilitino richieste in emergenza da parte dei terzi interessati.

Nota 4: la durata di una sospensione DOVREBBE essere limitata a un valore massimo prefissato e noto, per una uniformità di comportamento tra i vari certificatori.

f. qualora uno dei funzionari addetti al servizio di certificazione, sia esso dipendente del certificatore o di fornitori esterni, venga a conoscenza di condizioni che comportano la revoca o la sospensione di un certificato qualificato, egli attiva la procedura prevista per tale revoca o almeno per la sospensione;

g. il titolare viene avvisato dell'imminente e dell'avvenuta revoca o sospensione almeno nel caso in cui essa sia richiesta dal terzo interessato o dal certificatore stesso.

Nota 5: Anche se non richiesto dalla normativa è buona norma informare il titolare dell'avvenuta sospensione o revoca del suo certificato anche quando esse risultino richieste dal titolare stesso.

2. Su richiesta del valutatore emette certificati che gli consentano di effettuare le verifiche previste, ivi inclusa la revoca e la sospensione dei medesimi così come l'annullamento delle sospensioni.
3. Esibisce documentazione e verbali che dimostrino che quanto indicato al punto 1 sia effettivamente ottemperato.

8.10.3 Il valutatore

1. Verifica l'esistenza dei documenti e delle procedure di cui al paragrafo 8.10.2, compreso il contenuto dei log. In particolare, ma non esclusivamente, verifica l'esistenza di procedure che assicurino:
    a. l'effettiva autenticazione del richiedente di una revoca/sospensione;
    b. la segretezza del codice di emergenza anche quando utilizzato;
    c. le comunicazioni al titolare di un certificato, previste dalle normative, relative all'imminente e all'avvenuta revoca o sospensione.
2. Verifica che nelle CRL non risultino certificati sospesi per un periodo maggiore di quanto eventualmente indicato nel Manuale operativo.
3. Può richiedere certificati con cui verificare l'effettuazione delle procedure di sospensione e revoca e l'annullamento della sospensione.
4. Verifica che i certificati dei sistemi di validazione temporale non siano revocati a seguito della sostituzione delle chiavi di firma dei sistemi medesimi. Si veda anche il paragrafo 10.2
5. Verifica i verbali di cui al paragrafo 8.10.2.

8.11 Servizio di informazione sullo stato dei certificati

Finalità: Fornire alle parti interessate informazioni sullo stato dei certificati. Questo servizio può essere effettuato in tempo reale o essere basato su aggiornamenti dello stato delle revoche ad intervalli regolari di tempo.

8.11.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3 lettere g), h), i)

Art. 36. Revoca e sospensione dei certificati qualificati. – comma 3

DPCM 13/1/2004

Art. 17. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione. – commi 1, 2

Art. 21. Sospensione dei certificati qualificati. – comma 1

Art. 35. Formato dei certificati qualificati.

Art. 38. Manuale operativo. – commi 1, 2, 3, lettera m)

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 5

Art. 9. Verifica dei certificati – CRL

Art. 10. Verifica in tempo reale dei certificati – OCSP

Art. 11. Coerenza delle informazioni sulla revoca e sospensione dei certificati

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

h) modalità di accesso alle informazioni di revoca e di sospensione dei certificati;

8.11.2 Il certificatore

1. Esibisce documentazione e procedure operative che dimostrino che:
    a) il momento della pubblicazione della revoca o sospensione è registrato nel giornale di controllo e attestato da adeguato riferimento temporale;
    b) è rispettato l'intervallo tra due emissioni successive di CRL indicato nel Manuale operativo;
    c) le revoche o sospensioni vengono pubblicate nella prima CRL per la quale tale pubblicazione sia tecnicamente possibile;
    d) qualora la richiesta di revoca o sospensione di un certificato sia motivata da possibile compromissione della chiave privata corrispondente, la pubblicazione della relativa revoca o sospensione avviene tempestivamente;
    e) ove il certificatore si avvalga di sistemi on line di divulgazione dello stato dei certificati (OCSP), tali sistemi non forniscono informazioni difformi rispetto a quanto riportato dall'ultima CRL emessa compatibilmente con i tempi tecnici necessari.
2. Mette a disposizione del valutatore certificati emessi.
3. Su richiesta del valutatore emette appositamente certificati che gli consentano di effettuare le verifiche previste, ivi inclusa la revoca dei medesimi.

8.11.3 Il valutatore

1. Verifica l'esattezza della registrazione nel giornale di controllo, controllato come indicato al punto 1 del paragrafo 7.1.3, delle operazioni relative alla pubblicazione delle revoche nella CRL, compreso il momento della loro pubblicazione.
2. Verifica che l'intervallo tra la pubblicazione di due CRL consecutive non sia superiore a quanto indicato nel Manuale operativo.
3. Verifica la rispondenza delle CRL al formato e ai metodi di accesso indicati all'art. 9 della Deliberazione CNIPA 4/2005.
4. Può richiedere l'emissione di certificati di cui richiedere una sospensione (anche in emergenza) e revoca.
5. Verifica l'effettiva possibilità di accedere alle CRL e, ove del caso, agli OCSP responder del certificatore.
6. Ove il certificatore si avvalga di sistemi OCSP, verifica la loro rispondenza alla specifica pubblica RFC 2560 e che nei certificati sia valorizzata correttamente la estensione authorityInfoAccess secondo quanto indicato all'art. 4 comma 6 della Deliberazione CNIPA 4/2005.

7. Verifica la rispondenza delle CRL ai requisiti del Titolo V della Deliberazione CNIPA 4/2005.
8. Ove siano previsti più metodi di distribuzione delle informazioni sullo stato dei certificati, ivi inclusi diversi CRL Distribution Point e servizi OCSP, verifica che le informazioni provenienti dalle varie fonti siano coerenti tra loro.

Capitolo 9

Gestione e operatività del sistema di CA

9.1 Gestione della sicurezza

Finalità: Applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute, tra cui gli standard di sicurezza emessi da organismi internazionali.

Nota: Le misure indicate nello standard ISO/IEC 17799 sono ritenute atte ad ottenere una adeguata sicurezza dei sistemi informativi. Sono pertanto ritenute soddisfacenti le misure ad esso conformi.

9.1.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettere a, b, c, d

Dlgs 196/2003

Art. 31: "Obblighi di sicurezza"

1. *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Nel caso di soggetti pubblici si applica anche il seguente art. 22.3:

"*I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.*"

DPCM 13/1/2004

Art. 8. Generazione delle chiavi al di fuori del dispositivo di firma. – comma 3

Art. 9. Dispositivi sicuri e procedure per la generazione della firma. – comma 6

Art. 14. Generazione dei certificati qualificati. – comma 3

Art. 17. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione. – comma 3

Art. 21. Sospensione dei certificati qualificati. – comma 2

Art. 28. Sistema di generazione dei certificati qualificati. – commi 2, 4

Art. 30. Piano per la sicurezza. – comma 1, lettere n), o), p)

Art. 31. Giornale di controllo.

Art. 32. Sistema di qualità del certificatore.

9.1.2 Il certificatore

1. In base a quanto indicato nel Piano per la sicurezza depositato in CNIPA, relativamente a risultanze di Risk Assessment, contromisure, controlli aggiornati e procedure interne coerentemente adottate dovrebbe esibire Security Policy strategiche, di sistema, elementari, approvate dal Management e rese note al personale interessato. Ove alcuni rischi siano stati accettati dal certificatore, deve esserne esibita la formale accettazione integrata dalla relativa motivazione.

   Nota 1: il Risk Assessment dovrebbe essere periodicamente rivisto sotto la Responsabilità del Responsabile della sicurezza, in base all'evoluzione della tecnologia, ai risultati degli audit di sicurezza interni ed esterni, agli incidenti di sicurezza, all'evoluzione degli attacchi e alle vulnerabilità individuate. Le Security Policy dovrebbero essere aggiornate di conseguenza.

2. Esibisce procedure da cui emerga il rispetto dei requisiti del Dlgs 196/2003.

3. Conformemente con la raccomandazione indicata nella Nota del capitolo 9.1 è auspicabile che gli incidenti di sicurezza, attuali o potenziali, siano gestiti come indicato al capitolo 13 dello ISO/IEC 17799. Il certificatore dovrebbe quindi comunque esibire:

   a. una procedura, preferibilmente conforme con lo standard citato, per la gestione degli incidenti di sicurezza e dei punti deboli eventualmente individuati nel sistema di sicurezza, in cui siano chiaramente indicate almeno:

      i. le responsabilità individuali;

      ii. le informazioni da riportare relativamente ai singoli tipi di incidente e di punti deboli del sistema di sicurezza;

      iii. le misure da attuare per il ripristino dell'operatività a seguito di incidenti;

   b. i report sulla registrazione e gestione di questi incidenti attuali o potenziali al fine di dimostrare il conseguente adeguamento delle misure di sicurezza;

4. Esibisce documentazione comprovante la verifica almeno mensile dell'integrità del giornale di controllo.

5. Ove il valutatore lo richieda, gli consente l'accesso, debitamente controllato e registrato, se necessario utilizzando le funzionalità previste per gli auditor e gli ispettori, a funzioni, servizi, sistemi, locali, ecc. il cui accesso prevede, come da norme vigenti, la registrazione sul giornale di controllo. Ove del caso gli consente con pari modalità anche l'accesso alle sedi di fornitori esterni che svolgono mansioni per conto del certificatore.

6. Consente al valutatore l'accesso, con le funzionalità degli auditor e degli ispettori, al giornale di controllo.

7. Le procedure esibite dal certificatore devono essere conformi con quanto indicato nel Piano per la sicurezza.

   Nota 2: le norme tecniche indicate dallo ISO/IEC 17799 prevedono che almeno le attività più delicate siano svolte in regime di "dual control".

9.1.3 Il valutatore

1. Verifica che i rischi individuati dal Risk Assessment, riflessi nelle contromisure e nei controlli indicati nel Piano per la sicurezza, siano adeguatamente gestiti nelle procedure, conformemente con le Security Policy in vigore approvate dal Management e rese note al personale interessato, oppure che essi siano esplicitamente accettati dal Management stesso, nel qual caso verifica che le motivazioni di tale accettazione siano esposte chiaramente.

2. Verifica che esistano procedure aventi come obiettivo il rispetto dei requisiti del Dlgs 196/2003.

Nota: la valutazione di vigilanza sui certificatori qualificati non entra nel merito della adeguatezza di queste procedure a rispettare le norme di cui al Dlgs in questione, ma si limita a verificarne l'esistenza e l'applicazione.

3. Verifica l'esistenza di procedure per la gestione degli incidenti di sicurezza, attuali o potenziali, e verifica che esse siano preferibilmente conformi con la sostanza di quanto indicato nello ISO/IEC 17799.
4. Il valutatore verifica la corrispondenza delle misure adottate con gli incidenti verificatisi oppure con le risultanze dei Risk Assessment.
5. Verifica la documentazione comprovante che almeno ogni mese viene verificata l'integrità del giornale di controllo, come indicato al comma 5 dell'art. 31 del DPCM 13/1/2004.
6. Può chiedere di accedere, con mansioni di auditor o ispettore, a funzioni, servizi, sistemi, locali, ecc., anche di fornitori esterni del certificatore, il cui accesso comporta la registrazione sul giornale di controllo.
7. Verifica l'esattezza delle registrazioni nel giornale di controllo delle operazioni previste ai seguenti articoli del DPCM 13/1/2004: 8 comma 3, 9 comma 6, 14 comma 3, 17 comma 3, 21 comma 2, 28 comma 2, 28 comma 4.
8. Verifica che esistano verbali di auditing (interno o esterno) che attestino l'effettiva esecuzione e il rispetto delle procedure previste ai punti 2 e 3 del paragrafo 9.1.2.

9.2 Gestione degli asset

Finalità: Assicurare che dati, informazioni e altri asset siano adeguatamente protetti.

9.2.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettere d),

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere j), m)

DPCM 13/1/2004

Art. 30. Piano per la sicurezza. – comma 1, lettere h), m)

Art. 31. Giornale di controllo. – comma 1

Nota: A integrazione della normativa, che per sua natura non può scendere troppo in dettaglio, si fornisce di seguito a titolo esemplificativo un elenco non esauriente di possibili "asset" relativi all'attività di certificazione, impostato sviluppando quanto indicato nello ISO/IEC 17799:

- Sale macchine e chiavi o codici per accedervi;
- Armadi, casseforti e chiavi o codici per accedervi;
- Sistemi e password o chiavi fisiche per accedere al BIOS;
- Sistemi operativi dei computer e account abilitati con i relativi livelli di sicurezza;
- Reti LAN e WAN, relativi dispositivi e installazioni fisiche (router, firewall, IDS, IPS, cavedi, ecc.);
- Software della CA e vari tipi di utenza (master user, security officer, CRL user).
- Dispositivi crittografici e datakey, chiavi fisiche;
- Codici PIN e password.
- Supporti mobili e altre apparecchiature.
- Vari tipi di dati:
    - database e file, contratti, accordi, documentazione di sistema;

- ricerche documentali, manuali utente, procedure operative o di supporto;
- Business Continuity Plan, accordi ad esso relativi;
- Dati di audit;
- Tool di sviluppo, programmi di utilità.

9.2.2 Il certificatore

1. Anche se non è previsto esplicitamente dalla normativa, un certificatore, per operare con misure conformi con quanto indicato nello standard ISO/IEC 17799, dovrebbe:
    a. attribuire a ogni asset il corretto livello di criticità, in base alle sue finalità (Confidentiality, Integrity, Availability) e al suo livello di importanza; (ISO/IEC 17799 Capitolo 7.2)
    b. "*individuare chiaramente tutti gli "asset" di rilievo e redigerne un inventario che mantiene aggiornato*" (ISO/IEC 17799 Capitolo 7.1); questo inventario, redatto e tenuto aggiornato tenendo conto della classificazione di cui al punto precedente, dovrebbe elencare gli asset tenendo conto di quanto indicato nella Nota del paragrafo precedente;
    c. contraddistinguere ciascun asset di rilievo con un identificatore in base a criteri e a procedure stabiliti che ne attribuiscano le relative responsabilità; ad esempio: gli asset materiali con un'etichetta o un contrassegno ad essi applicati ove possibile, quelli immateriali, come ad esempio le informazioni, con un contrassegno applicato al supporto che le contiene e che faccia riferimento al contenuto;
    d. attribuire la responsabilità di ogni elemento inventariato a una persona o a una funzione (ISO/IEC 17799 Capitolo 7.2), in questo secondo caso il responsabile della funzione diventa automaticamente responsabile dell'asset;
    e. ove del caso agli elementi inventariati dovrebbero corrispondere specifiche misure di sicurezza.
2. L'inventario e quant'altro descritto al precedente punto 1 dovrebbe essere attuato almeno per i dispositivi di sicurezza la cui descrizione è richiesta nel Piano per la sicurezza.
3. Per quegli asset per i quali esistano Security Policy specifiche, esibisce procedure che ne assicurino l'ottemperanza.
4. Esibisce procedure di disaster recovery e di gestione degli incidenti di sicurezza di minor rilievo atte ad assicurare la conservazione e leggibilità, per i venti anni indicati dal Dlgs 159/2006, delle informazioni relative ai certificati, ovunque esse siano registrate.
5. Consente al valutatore di effettuare le verifiche del caso in situ.
6. Ove tali asset siano situati presso le sedi di fornitori esterni assicura al valutatore la possibilità di accedervi.

9.2.3 Il valutatore

1. Verifica l'esistenza dell'inventario degli asset, come indicato al punto 1 del paragrafo 9.2.1, con i relativi identificatori e assegnatari, in particolar modo per i dispositivi di sicurezza la cui descrizione è richiesta nel Piano per la sicurezza.
2. Per quegli asset per i quali esistano Security Policy specifiche verifica l'esistenza di procedure che ne assicurino l'ottemperanza, verificando, ove del caso, i relativi verbali.
3. Effettua, ove del caso, verifiche in situ sugli asset onde verificare che le procedure che li riguardano siano rispettate.
4. Prende atto, ove del caso, dell'esistenza di procedure di gestione dei disastri, così come di quelle per la gestione degli altri incidenti di sicurezza, e della dichiarazione del certificatore che esse assicurano l'esigenza di garantire integrità, conservazione e leggibilità delle informazioni relative ai certificati qualificati per il periodo di venti anni indicato dal Dlgs 159/2006.

9.3 Gestione del personale

Finalità: impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; avvalersi, inoltre, di personale affidabile e pienamente consapevole dei propri compiti e responsabilità.

Nota: quanto segue si applica al personale, esecutivo e manageriale, sia del certificatore sia di eventuali suoi fornitori di servizi di certificazione.

9.3.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettera b)

Art. 29. Accreditamento. – comma 2

DPCM 13/1/2004

Art. 11. Informazioni riguardanti i certificatori. – comma 1, lettera l)

Art. 30. Piano per la sicurezza. – comma 1, lettere d), e)

Art. 33. Organizzazione del personale del certificatore.

Art. 34. Requisiti di competenza ed esperienza del personale.

Circolare 6 settembre 2005, n. 48

[omissis] alla domanda deve essere allegata la seguente documentazione:

p) una relazione sulla struttura organizzativa, debitamente sottoscritta dal legale rappresentante;

Nota : è implicito che il contravvenire a disposizioni operative e di sicurezza possa comportare l'applicazione al personale delle sanzioni previste dalle norme in vigore.

9.3.2 Il certificatore

1. Mette a disposizione del valutatore il personale indicato nella Relazione sulla struttura organizzativa consegnata a CNIPA per le verifiche previste.
2. Per ciascuna persona esibisce documentazione da cui emerga che essa ha preso formalmente conoscenza delle proprie mansioni e responsabilità coerenti con le Security Policy in essere. In particolare, ove del caso e per ruoli specifici, tra le responsabilità dovrebbero essere indicati il vincolo alla riservatezza e le eventuali modalità con cui esso deve essere assicurato anche dopo la cessazione dall'incarico.
3. Esibisce documentazione relativa ad un'adeguata informativa al personale interno, e una analoga clausola degli accordi con i fornitori esterni, sul fatto che violazioni delle disposizioni operative e di sicurezza possono essere sanzionate in base alle normative vigenti.
4. Esibisce documentazione atta a dimostrare l'effettivo possesso da parte del personale dei requisiti di competenza, esperienza, anche nel campo della sicurezza, previsti dalla normativa vigente.
5. Esibisce documentazione atta a dimostrare l'erogazione al personale in questione di opportuno e aggiornato addestramento sulla parte di propria competenza, ivi inclusi gli aspetti relativi alla sicurezza.
6. Esibisce procedure che indichino le misure da adottare quando una persona addetta ai servizi di certificazione lascia l'incarico, in maniera pianificata o imprevista, con particolare attenzione al caso di cessazione conflittuale del rapporto di lavoro. Esse dovrebbero prevedere almeno che, con tempestività, si abbia la restituzione del materiale affidato in relazione all'erogazione dei servizi di certificazione, l'eliminazione dei relativi account o, ove del caso, almeno la disattivazione dei privilegi relativi. Esibisce, ove del caso, documentazione comprovante l'avvenuta esecuzione di tali procedure.

7. Ove richiesto dal valutatore, consente l'esecuzione di procedure documentate per verificarne la dimestichezza da parte del personale a ciò deputato.

Nota: anche se non è chiaramente indicato in nessuna norma, è altamente raccomandato che la medesima persona non sia incaricata di svolgere operazioni all'interno dei servizi di certificazione in situazione di conflitto di interesse con altre mansioni da lui rivestite.

9.3.3 Il valutatore

1. Verifica, eventualmente a campione, l'esistenza del personale indicato nella Relazione sulla struttura organizzativa consegnata a CNIPA.
2. Verifica l'effettiva attribuzione al personale indicato nella Relazione sulla struttura organizzativa consegnata a CNIPA delle responsabilità previste dall'art. 33 del DPCM 13/1/2004.
3. Verifica che la documentazione esibita dia evidenza:
    a) che ogni persona interessata sia stata messa a conoscenza delle proprie responsabilità connesse con lo specifico incarico e che in caso di violazione di disposizioni operative e di sicurezza possono essere applicate le sanzioni previste dalla normativa vigente;
    b) del possesso da parte della persona dei requisiti di competenza ed esperienza previsti dalla normativa in vigore;
    c) dell'erogazione al personale del necessario addestramento;
    d) della gestione della cessazione dagli incarichi.
4. Verifica che dalla documentazione esibita dal certificatore non risultino evidenti situazioni di conflitto di interesse tra le cariche ricoperte da una stessa persona.
5. Verifica ove del caso, dalla documentazione esibita e da altre evidenze, che le procedure previste per la cessazione di una persona da incarichi connessi con la CA siano state effettivamente eseguite.
6. Può richiedere l'esecuzione di procedure documentate per verificarne la dimestichezza da parte del personale a ciò deputato.

9.4 Sicurezza fisica

Finalità: assicurare il controllo degli accessi fisici ai servizi critici e rendere minimi i rischi fisici per gli asset.

9.4.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettere d)

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera m)

DPCM 13/1/2004

Art. 8. Generazione delle chiavi al di fuori del dispositivo di firma. – commi 1, 2, 3

Art. 28. Sistema di generazione dei certificati qualificati. – commi 1, 2

Art. 30. Piano per la sicurezza. – comma 1, lettere a), b), c), m)

9.4.2 Il certificatore

1. Mette il valutatore in grado di accedere, nel rispetto delle misure di sicurezza, alle infrastrutture fisiche e ai sistemi utilizzati per la prestazione dei servizi di certificazione.

   Nota: si veda anche quanto indicato nella Nota 1: del paragrafo 7.1.2.

2. Esibisce documentazione sulle modalità di protezione della copia master del registro dei certificati.
3. Esibisce le procedure che governano l'accesso ai locali ove sono situati i sistemi in questione, la loro comunicazione agli interessati e l'elenco delle persone autorizzate ad accedervi.
4. Esibisce le procedure di gestione dei supporti informatici, deputati a contenere informazioni relative alle attività di certificazione, volte a proteggere essi stessi e il loro contenuto da accessi non autorizzati (anche quando essi vengono eliminati – sanitisation) e da incidenti quali: mancanza improvvisa di tensione elettrica, blocco del sistema di aria condizionata, allagamenti, ecc.
5. Esibisce i verbali di esecuzione delle procedure di gestione dei supporti informatici in questione.
6. Esibisce gli inventari dei supporti informatici in questione.
7. Esibisce verbali di auditing interno ed esterno concernenti ispezioni sui locali in questione.

Nota: le misure di sicurezza indicate dallo ISO/IEC 17799, alle quali è auspicato che il certificatore si adegui, prevedono, tra l'altro, che:

- quanto utilizzato per elaborazioni critiche o delicate sia allocato in aree sicure, protetto da perimetri di sicurezza ben definiti, protetto da accessi non autorizzati, da danni e interferenze, con barriere e controlli di accesso appropriati;
- siano attuate misure preventive contro eventi quali "*incendi, allagamenti, terremoti, esplosioni, rivolte, altri disastri naturali o provocati dall'uomo*"[4];
- esistano misure per ovviare a inconvenienti quali prolungata mancanza di acqua o di energia elettrica o di riscaldamento o condizionamento;
- locali, sistemi e reti adibiti alla prestazione di servizi ad alto contenuto di sicurezza siano realizzati e collocati in modo tale da evitare:
  i. condizioni ambientali sfavorevoli sia per le persone sia per le attrezzature,
  ii. l'acquisizione indebita di informazioni mediante lettura, anche dall'esterno del locale, degli schermi di computer e dei display di unità varie,
  iii. l'acquisizione indebita di informazioni riservate captando le emanazioni magnetiche, di campo elettrico o simili; quest'ultimo aspetto deve riguardare anche i cavedi ove transitano i collegamenti di rete.
- almeno le attività più delicate siano svolte in regime di "dual control".

9.4.3 Il valutatore

1. Verifica che sistemi e reti utilizzati per l'erogazione dei servizi di certificazione, o quanto meno il sistema di generazione dei certificati, siano allocati entro locali che risultino (dai verbali di auditing interno ed esterno) fisicamente isolati e protetti contro: accessi non autorizzati, acquisizione indebita di informazioni riservate, eventi quali "*incendi, allagamenti, terremoti, esplosioni, rivolte, e altri disastri naturali o provocati dall'uomo*".

   Nota: Ancorché non richiesto esplicitamente dalla normativa è buona norma allocare il sistema "Master" del registro dei certificati in locali isolati e proteggerlo adeguatamente contro i rischi di interferenze ed intercettazioni.

2. Verifica che le procedure che governano l'accesso ai locali protetti e ai sistemi utilizzati per i servizi di certificazione prevedano l'accesso alle sole persone autorizzate di cui ha ricevuto l'elenco.

[4] ISO/IEC 17799 capitolo 9.1.4

3. Verifica i risultati dei verbali di auditing e, qualora vi siano state valutazioni sfavorevoli, verifica che siano state intraprese adeguate misure correttive.
4. Verifica l'esistenza di evidenze dell'esecuzione delle procedure di gestione dei supporti informatici deputati a contenere informazioni relative alle attività di certificazione.
5. Verifica, se del caso a campione, la rispondenza degli inventari dei supporti informatici in questione alla situazione reale.
6. Può effettuare tentativi di accesso alle varie infrastrutture fisiche e ai sistemi utilizzati per la prestazione dei servizi di certificazione onde verificare se i requisiti di controllo accessi siano rispettati.
7. Verifica se dalle registrazioni del giornale di controllo, sottoposto a verifica come indicato al punto 1 del paragrafo 7.1.3, risulta che l'accesso ai locali, così come l'inizio di ogni sessione di lavoro, è controllato e registrato.

9.5 Altri aspetti della gestione operativa

Finalità: assicurare che i sistemi di erogazione dei servizi di certificazione siano protetti da attacchi, dispongano di capacità elaborativa atta a fornire con continuità il servizio richiesto rendendo minimo il rischio di interruzioni di servizio anche in caso di incidente, sottoponendo il tutto a verifiche di auditing..

9.5.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettere c), d)

DPCM 13/1/2004

Art. 11. Informazioni riguardanti i certificatori. – comma 1, lettera l)

Art. 30. Piano per la sicurezza. – comma 1, lettere e), n), o), p)

Art. 33. Organizzazione del personale del certificatore. – comma 1, lettere a), l)

Nota: Anche se la normativa giuridica non entra molto nei dettagli di sicurezza, è altamente opportuno che le misure di sicurezza normalmente previste (si veda ISO/IEC 17799) siano rispettate anche dai certificatori italiani. In particolare:

1. misure di prevenzione di attacchi tramite codici dannosi quali virus, trojan horse, ecc; tra queste misure vanno incluse le procedure per apportare tempestivamente e in modo affidabile le "patch" di sicurezza rilasciate dai produttori del SW utilizzato;
2. strumenti di contrasto di altri tipi di attacco, quali intrusioni nella rete e nelle applicazioni, provenienti sia dall'esterno sia dall'interno della rete, ecc.;
3. gestione degli incidenti, dal reporting fino alla possibilità di continuare a fornire i servizi anche in caso di disastro;
4. gestione dei supporti informatici: danneggiamenti, furti, controllo accessi, obsolescenza tecnica, deterioramento, eliminazione previa sanitisation (distruzione dei dati ivi registrati);
5. system capacity planning;
6. assegnazione dei ruoli ad addetti che non rivestano contemporaneamente compiti in situazione di conflitto di interesse;
7. addestramento degli addetti.

9.5.2 Il certificatore

1. Esibisce documentazione da cui emerga che gli aspetti di sicurezza indicati al capitolo 9.5.1 sono formalmente assegnati a Responsabili individuati tra quelli indicati nella Relazione sulla Struttura organizzativa, e/o quelli indicati nel Piano della sicurezza.
2. Esibisce la documentazione delle configurazioni dei sistemi utilizzati per la generazione dei certificati, per il registro dei certificati, per le reti impiegate, ecc. da cui risulti l'adozione di misure di contrasto a codice dannoso e ad attacchi provenienti sia dall'esterno sia dall'interno della rete; in particolare dovrebbe emergere una procedura che preveda una tempestiva e affidabile applicazione delle "patch" di sicurezza rilasciate dai produttori del SW utilizzato.
3. Esibisce le procedure in vigore, incluse le specifiche responsabilità, atte a tenere i responsabili prontamente aggiornati su problemi concernenti la sicurezza: mailing list, contatti con Computer Emergency Response Team, ecc.
4. Esibisce le procedure in vigore per la segnalazione e la gestione degli incidenti e dei disastri, ove del caso depurate dagli aspetti più riservati, purché sia consentito al valutatore di effettuare le necessarie verifiche sulla reale operatività delle procedure.
5. Esibisce le procedure in vigore per la gestione dei supporti informatici, deputati a contenere informazioni relative alle attività di certificazione, che comprendano anche verifiche sul loro livello di degrado e prevenzione della loro obsolescenza tecnica.
6. Esibisce le procedure in vigore per la revisione almeno periodica della capacità elaborativa.
7. Esibisce verbali di auditing interno e/o esterno da cui risulti la effettiva corrispondenza delle configurazioni operative con quelle descritte nella documentazione di cui al punto 2.
8. Esibisce, ove possibile, verbali di incidenti di sicurezza o di disastri da cui risulti che le procedure esibite al punto 4 sono state effettivamente applicate.
9. Esibisce verbali da cui emergano l'effettivo adeguamento della capacità elaborativa a seguito delle procedure di revisione di cui al punto 6 e il rispetto delle procedure per la gestione dei supporti informatici.
10. Consente al valutatore di effettuare verifiche dirette atte a riscontrare se i requisiti di sicurezza indicati alla Nota del capitolo 9.5.1 sono stati realizzati.

Nota: per quanto è applicabile, le attività relative alle misure di sicurezza devono essere coerenti con il Risk Assessment indicato nel Piano per la sicurezza. Per un maggior dettaglio circa le modalità di effettuazione e gestione del Risk Assessment e la gestione dei disastri vedere il paragrafo 10.8

9.5.3 Il valutatore

1. Verifica l'esistenza delle procedure e della documentazione di cui al paragrafo 9.5.2; in particolare, ma non esclusivamente, verifica l'esistenza di procedure atte a mantenere aggiornato il personale sui problemi di sicurezza.
2. Verifica che dai verbali esibiti risulti:
    a. che le configurazioni esibite per sistemi e reti sono effettivamente corrispondenti a quelle operative; può effettuare personalmente verifiche di questo tipo;
    b. che gli eventuali incidenti di sicurezza o disastri siano stati gestiti come previsto dalle rispettive procedure;
    c. l'effettiva esecuzione delle procedure di revisione della capacità elaborativa e il rispetto delle procedure per la gestione dei supporti informatici; può effettuare personalmente verifiche per controllare l'effettivo adeguamento delle configurazioni.
3. Può effettuare verifiche dirette atte a riscontrare il rispetto dei requisiti di sicurezza indicati alla Nota del capitolo 9.5.1.

9.6 Gestione accesso ai sistemi

Finalità: assicurare che ai sistemi del certificatore possano accedere solo persone debitamente autorizzate.

9.6.1 Normativa

Dlgs 196/2003

Art. 31: "Obblighi di sicurezza"

2. *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Nel caso di soggetti pubblici si applica anche il seguente art. 22.3:

"*I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.*"

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera m)

DPCM 13/1/2004

Art. 8. Generazione delle chiavi al di fuori del dispositivo di firma. – commi 2, 3,

Art. 28. Sistema di generazione dei certificati qualificati. – commi 1, 2, 3

Art. 38. Manuale operativo. – comma 3, lettera p)

9.6.2 Il certificatore

1. Esibisce documentazione da cui emerga che la propria rete destinata alla fornitura dei servizi di certificazione è adeguatamente protetta da accessi non autorizzati da parte di personale interno ed esterno (ad esempio: mediante autenticazione, Firewall, IDP, IPS, utilizzo di secure channel per il personale autorizzato, cifratura per i dati personali sensibili, ecc.).
2. Esibisce le procedure per la registrazione, gestione e rimozione dei privilegi del personale all'accesso a sistemi, locali e reti.
3. Esibisce l'elenco delle persone autorizzate ad accedere a sistemi, locali e reti.
4. Ove del caso esibisce le regole per la composizione delle password e le misure per verificarne l'effettivo rispetto.
5. Esibisce procedure da cui emerga la protezione dei sistemi utilizzati per l'erogazione dei propri servizi (generazione dei certificati, registro dei certificati, sistemi OCSP, ecc.).
6. Esibisce documentazione da cui emerga che almeno le attività più delicate di gestione della rete sono svolte in regime di "dual control".
7. Esibisce procedure che prevedano una regolare ispezione dei log e registri, incluso il giornale di controllo, dei sistemi utilizzati e dei dispositivi messi a protezione della rete da intrusioni, da cui risultino gli accessi, i tentativi di accesso non autorizzato, i codici identificativi degli autori dell'accesso o dei tentativi di accesso, come anche le misure intraprese a seguito dei tentativi di intrusione e accesso non autorizzato. E' auspicabile che siano effettuati anche penetration test.
8. Esibisce verbali di auditing interno o esterno da cui emerga il rispetto della configurazione prevista per gli strumenti utilizzati per prevenire intrusioni nella rete e l'effettiva periodica ispezione dei log e registri interessati.

9. Assiste il valutatore qualora questi ritenga opportuno effettuare tentativi di accesso non autorizzato.

9.6.3 Il valutatore

1. Verifica l'esistenza delle procedure indicate al paragrafo 9.6.2.
2. Verifica che dalla documentazione di cui paragrafo 9.6.2 emerga il rispetto delle misure e procedure ivi indicate.
3. Verifica che dai verbali di auditing interno o esterno emerga il rispetto delle procedure indicate al capitolo 9.6.2. E' auspicabile che l'auditor o l'ispettore abbia effettuato anche penetration test.
4. Verifica alcune registrazioni del log allo scopo di verificare se persone, non indicate dal certificatore come autorizzate, abbiano avuto accesso a sistemi, locali e reti, e che almeno le attività più delicate siano svolte in regime di "dual control".
5. Può effettuare, con l'assistenza del personale del certificatore, tentativi di accesso a locali, sistemi e reti per verificarne l'effettiva rispondenza della protezione a quanto dichiarato.

9.7 Utilizzo e manutenzione dei sistemi del certificatore

Finalità: utilizzare sistemi affidabili e prodotti protetti da alterazioni e che forniscano sicurezza tecnica e crittografica ai procedimenti di cui sono oggetto.

9.7.1 Normativa

Dlgs 82/2005

Art. 27. Certificatori qualificati. – comma 2, lettera d)

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera m)

DPCM 13/1/2004

Art. 27. Requisiti di sicurezza dei sistemi operativi.

9.7.2 Il certificatore

1. Esibisce documentazione da cui emerga l'utilizzo di sistemi e prodotti conformi con requisiti e certificazioni di sicurezza indicati nella normativa, siano essi disponibili sul mercato o realizzati appositamente.
2. Esibisce le procedure di "hardening" dei sistemi e, ove del caso, dei dispositivi utilizzati.
3. Esibisce le procedure di change management di sistemi, dispositivi e reti, che assicurino la valutazione, il collaudo e l'accettazione dei medesimi, o delle modifiche ad essi apportate, prima che essi o le relative modifiche divengano operative.
4. Esibisce verbali di installazione di sistemi, dispositivi e reti da cui risulti sia un'adeguata fase di prova e collaudo prima dell'attivazione in ambiente operativo, sia, ove del caso, l'esecuzione delle procedure di hardening.
5. Esibisce verbali di auditing che confermino l'esecuzione delle procedure di cui ai punti precedenti e, ove del caso, la verifica di assenza di funzioni non necessarie da sistemi e dispositivi.
6. Consente al valutatore di accedere ai sistemi, nel rispetto delle procedure di sicurezza, per verificare la rispondenza alle misure di hardening.

Nota: anche se non previsto esplicitamente dalla normativa, le normali misure di sicurezza (si veda ISO/IEC 17799) richiedono l'uso di ambienti elaborativi separati per lo sviluppo e test, per il collaudo e per la produzione.

9.7.3 Il valutatore

1. Verifica l'esistenza della documentazione e delle procedure indicate al capitolo 9.7.2.
2. Verifica l'esistenza dei verbali di installazione di cui al punto 4 del paragrafo 9.7.2.
3. Verifica l'esistenza dei verbali di auditing di cui al punto 5 del paragrafo 9.7.2.
4. Può effettuare verifiche sull'assenza da sistemi e dispositivi di funzioni non necessarie, in conformità con la procedura di hardening esibita dal certificatore.

9.8 Business Continuity management

Finalità: assicurare che in caso di disastro le operazioni siano riprese quanto prima, entro i termini dichiarati nel Piano per la sicurezza; la compromissione della chiave privata di firma del certificatore dovrebbe essere trattata alla stregua di un disastro.

9.8.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – commi 2, 3, lettere g), h), i), j)

DPCM 13/1/2004

Art. 7. Conservazione delle chiavi. – comma 2

Art. 26. Revoca dei certificati relativi a chiavi di certificazione.

Art. 30. Piano per la sicurezza. – comma 1, lettere i), l), m)

Nota: anche se non esplicitamente indicato nella normativa, la compromissione degli algoritmi o di chiavi di lunghezza pari a quella delle chiavi utilizzati dal certificatore o dai titolari deve essere trattato in modo tale da consentire una tempestiva informazione ai titolari dell'evento e una adeguata sostituzione delle chiavi o dell'algoritmo interessati.

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

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

9.8.2 Il certificatore

1. Esibisce, a eventuale integrazione di quanto indicato nel Piano per la sicurezza, il piano di gestione di incidenti e disastri, approvato dal management, redatto per le proprie attività e per quelle dei suoi fornitori relative sia alla certificazione, sia alla conservazione della relativa documentazione, inclusi i dati personali, che indichi:
    a. la metodologia di risk assessment adottata relativamente alle attività di certificazione;
    b. il criterio di definizione dei livelli di rischio accettabili e come individuarli;

c. l'individuazione dei rischi di interruzione del servizio correlati ai vari asset (minacce, vulnerabilità e conseguenze sui servizi – impact analysis);

d. la valutazione del rischio (probabilità che si verifichi, livello, valutazione della possibilità di accettare o di trasferire il rischio).

2. Esibisce documentazione da cui risulti che le contromisure adottate sono conformi con quanto indicato nel Piano per la sicurezza, in particolare:

   a. le misure adottate (piano di manutenzione HW e SW, duplicazione di attrezzature elaborative, dati, reti e servizi ausiliari, ecc.) per prevenire interruzioni del servizio causate da malfunzionamenti tecnici, operativi, da disfunzioni dei servizi ausiliari (quali mancata o incontrollata distribuzione di acqua, energia elettrica, gas, ecc.) verificatisi nel sito principale, e quanto previsto nei casi di disastro;

   b. la configurazione del sito, o dei siti, di disaster recovery e di quelli di storage backup e i relativi controlli di accesso, i quali devono essere congrui con le esigenze di sicurezza e con quella di far ripartire il servizio nel più breve tempo possibile;

      Nota 1: al fine di accelerare la ripartenza può essere buona norma conservare presso il sito di disaster recovery copia delle chiavi private di certificazione, nel rispetto dei requisiti di sicurezza indicati all'art. 7 comma 2 del DPCM 13/1/2004.

   c. le attività da svolgere ove necessario:

      i. per ripristinare le operazioni presso il sito di disaster recovery;

      ii. per ricostruire i dati eventualmente distrutti, presso sia il sito principale sia quello di disaster recovery, utilizzando le copie di back up disponibili e gestendo i dati eventualmente creatisi dall'ultimo salvataggio e non ancora conservati;

   d. il tempo massimo per il restart a seconda dei tipi di disastro o incidente;

   e. le fasi preparatorie, descritte in modo dettagliato, che prevedano anche una sistematica copia in almeno un sito di backup dei dati relativi a tutta la vita dei certificati, del registro dei certificati, dei dati di registrazione dei titolari, e di quant'altro necessario a proseguire le operazioni;

      Nota 2: I requisiti dell'art. 32 comma 3. punti g) e h) del Dlgs 82/2005 sottintendono anche una continuità di servizio dell'elenco dei certificati revocati e sospesi, onde agevolare la verifica delle firme. Ne deriva che di tale elenco è altamente auspicabile che siano attive più copie "shadow" che consentano quanto meno la consultazione delle CRL emesse anche nel caso in cui il sito principale non sia agibile.

      Nota 3: I dati relativi ai titolari devono essere conservati per almeno per 20 anni.

   f. gli incarichi affidati inequivocabilmente al personale e il loro addestramento al riguardo;

   g. l'attribuzione al personale dei privilegi di accesso e attivazione in maniera adeguata a consentire un ritorno all'operatività nei tempi dichiarati a CNIPA;

   h. modalità e frequenza delle prove di restart dei vari aspetti del piano, dal semplice ripristino dei dati a partire dalle copie di back up fino all'attivazione in emergenza delle sedi di disaster recovery;

   i. le modalità per la revisione del piano stesso.

   Nota 4: da questa documentazione potranno, ove del caso, essere eliminati gli aspetti più riservati, purché sia possibile al valutatore effettuare le necessarie verifiche di reale operatività delle procedure.

3. Esibisce, ove sia trascorso un tempo adeguato da richiedere l'effettuazione delle prove di gestione del restart, i relativi verbali.

4. Esibisce, ove sia trascorso un tempo adeguato da richiedere l'effettuazione della revisioni del piano di gestione incidenti e disastri, i relativi verbali..

5. Esibisce verbali di auditing interno o esterno che dimostrino l'effettiva aderenza dell'organizzazione del certificatore al piano di gestione di incidenti e disastri.

6. Il caso di compromissione delle chiavi di firma del certificatore deve essere incluso nel piano di gestione dei disastri e deve essere conforme con il requisito dell'art. 26 del DPCM 13/1/2004.
7. Il caso di compromissione degli algoritmi e della lunghezza di chiavi utilizzati dal certificatore deve essere assimilato a quello di compromissione della chiave di firma del certificatore.
8. Il caso di compromissione degli algoritmi e della lunghezza delle chiavi utilizzati dai titolari deve essere incluso nel piano di gestione disastri. In tale caso si deve prevedere almeno una informazione tempestiva e con mezzi durevoli, nei confronti dei titolari e di coloro che utilizzino i certificati emessi dal certificatore, che riguardi le possibili conseguenze e le misure da adottare.

9.8.3 Il valutatore

1. Verifica l'esistenza e attuazione del piano di gestione incidenti e disastri, e la sua corrispondenza con quanto consegnato a CNIPA nel Piano per la sicurezza, e di quant'altro indicato al riguardo nel paragrafo 9.8.2.
2. Verifica, ove del caso, l'esistenza di verbali di revisione del piano di gestione incidenti e disastri previsti al paragrafo 9.8.2.
3. Verifica i verbali di auditing previsti al paragrafo 9.8.2.
4. Può verificare l'effettiva esistenza e predisposizione delle misure di prevenzione incidenti e dei siti di Disaster Recovery e di storage backup, come anche delle relative procedure esecutive di dettaglio.
5. Verifica che le misure adottate circa la disponibilità dell'elenco dei certificati revocati e sospesi e la ripresa delle operazioni siano conformi con i tempi comunicati a CNIPA per i casi di disastro.
6. Verifica, ove del caso, l'esistenza di verbali di effettuazione di prove di restart e dei verbali di auditing citati al capitolo 9.8.2.

9.9 Conservazione delle informazioni relative ai certificati qualificati

Finalità: assicurare che la documentazione relativa ai certificati e ai loro titolari sia conservata secondo quanto indicato nel Dlgs 82/2005.

9.9.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettera j)

9.9.2 Il certificatore

1. Esibisce procedure per la conservazione e la protezione da accessi non autorizzati di quanto indicato all'art. 32 comma 3 lettera j) del Dlgs 82/2005 per il periodo di venti anni ivi indicato.
2. Esibisce verbali da cui risulti l'esecuzione delle procedure di cui al punto 1.
3. Esibisce la documentazione che venga richiesta dal valutatore.

9.9.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al capitolo 9.9.2.
2. Può richiedere l'esibizione di documenti relativi ai titolari alla cui conservazione il certificatore è tenuto.

Capitolo 10

Servizio di marcatura temporale

Finalità: il certificatore accreditato presso CNIPA deve disporre di un servizio di emissione di marche temporali affidabile conforme con la normativa vigente.

10.1 Sistema di generazione delle marche temporali e relativi locali

Finalità: il certificatore deve garantire che le marche temporali siano generate in un ambiente sicuro.

10.1.1 Normativa

Dlgs 82/2005

Art. 20. Documento informatico. – comma 3

DPCM 13/1/2004

Art. 2. Ambito di applicazione. – comma 4

Art. 30. Piano per la sicurezza. – comma 1

Art. 33. Organizzazione del personale del certificatore. – commi 1, lettera m), 2, lettera b)

Art. 34. Requisiti di competenza ed esperienza del personale.

Art. 44. Validazione temporale. – comma 2

Art. 48. Precisione dei sistemi di validazione temporale.

Art. 49. Sicurezza dei sistemi di validazione temporale.

Art. 50. Registrazione delle marche generate. – comma 1

Circolare 6 settembre 2005, n. 48

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

[omissis]

o) descrizione del sistema di validazione temporale adottato;

10.1.2 Il certificatore

1. Ove il servizio di marcatura temporale sia installato ed operante sotto il diretto controllo del certificatore:
    a) Esibisce procedure da cui risulti l'attuazione di misure di sicurezza e organizzative analoghe a quelle attuate per la emissione e gestione dei certificati, come indicato nel Manuale Operativo e nel Piano per la sicurezza.
    b) Consente al verificatore, sotto la supervisione di proprio personale addetto e nel rispetto delle norme indicate nel Piano della Sicurezza, l'accesso ai locali e ai sistemi dove sono gestiti i TSS, il registro delle marche temporali emesse, il registro operativo del sistema di validazione temporale.

c) Esibisce documentazione atta a dimostrare l'esistenza e operatività del/dei TSS a partire dall'inizio dell'attività di certificatore accreditato, quali:

   i. registro delle marche temporali emesse,

   ii. registro operativo del sistema di validazione temporale

   Di questi registri esibisce, in particolare, le misure adottate per renderli non modificabili.

d) Esibisce documentazione che fornisca evidenza del corretto funzionamento delle procedure che garantiscono la conformità del riferimento temporale riportato nel TST alle norme in vigore.

e) Esibisce documentazione che dimostri che il sistema di marcatura temporale è stato verificato conforme alle norme previste dall'art. 49 comma 4 del DPCM 13/1/2004.

f) Mette a disposizione del verificatore:

   i. i dati del registro delle marche temporali di cui all'art. 50 del DPCM 13/1/2004 e del registro operativo di cui all'art. 49 comma 1 del DPCM 13/1/2004 (in sola lettura);

   ii. il responsabile del sistema di marcatura temporale per fornire assistenza al valutatore;

g) Su richiesta del valutatore produce e rende disponibili marche temporali onde effettuare i controlli necessari.

2. Ove il servizio di marcatura temporale sia gestito da altro certificatore accreditato, come dichiarato nella documentazione depositata presso CNIPA, esibisce la relativa documentazione contrattuale.
3. Esibisce le procedure fornite ai titolari per la richiesta di TST e quelle fornite a tutti gli utenti per la loro verifica.
4. Esibisce le eventuali procedure con cui gli utenti possono richiedere la verifica delle marche temporali conservate.

   Nota: è da ritenere che, nel caso di compromissione della chiave di firma di un TSS, i detentori di un TST emesso con tale chiave richiedano in massa la verifica dei TST in questione conservati presso il certificatore. E' quindi auspicabile che il certificatore abbia pronta una procedura da attivare in caso di tale incidente.

10.1.3 Il valutatore

1. Ove il servizio di marcatura temporale sia installato ed operante sotto il diretto controllo del certificatore:
   a. Verifica la rispondenza del sistema di validazione temporale alla descrizione datane dal certificatore nella documentazione depositata in CNIPA come richiesto dalla Circolare CNIPA 48/2005.
   b. Verifica la relativa documentazione e i relativi dati di cui al paragrafo 10.1.2..
   c. Verifica l'esistenza della dichiarazione di conformità alle norme di cui all'art. 49 comma 4 del DPCM 13/1/2004.
   d. Verifica l'esistenza e l'integrità del registro delle marche temporali e del registro operativo.
   e. Può richiedere di accedere, nel rispetto delle norme di sicurezza, ai locali che ospitano i TSS;
2. Ove il servizio di marcatura temporale sia gestito da altro certificatore accreditato, dichiarato nella documentazione depositata presso CNIPA, verifica l'esistenza della relativa documentazione contrattuale.
3. Può richiedere l'emissione di marche temporali, nel rispetto delle procedure fornite ai titolari, per effettuarvi i controlli necessari con le procedure fornite a tutti gli utenti per la loro verifica.
4. Può verificare l'esistenza e l'efficacia della procedura con cui gli utenti possono richiedere la verifica delle marche temporali conservate dal certificatore.

10.2 Generazione e gestione di chiavi e certificati dei TSS e delle CA relative

Finalità: il certificatore deve garantire che le chiavi per l'emissione delle marche temporali siano generate sotto adeguato controllo e che chiavi e certificati di certificazione siano generati con modalità analoghe a quelle previste per chiavi e certificati di certificazione per i sistemi che emettono certificati qualificati.

Nota: i certificati dei TSS devono essere rilasciati utilizzando chiavi di certificazione diverse da quelle utilizzate per emettere i certificati qualificati.

10.2.1 Normativa

DPCM 13/1/2004

Art. 4. Caratteristiche generali delle chiavi per la creazione e la verifica della firma. – commi 4, lettera c), 5, 7

Art. 5. Generazione delle chiavi.

Art. 46. Chiavi di marcatura temporale.

Art. 47. Gestione dei certificati e delle chiavi.

Art. 53. Norme transitorie.

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 3

Art. 7. Uso delle estensioni nei certificati di marcatura temporale

10.2.2 Il certificatore

1. Esibisce documentazione che dimostri che le chiavi di certificazione utilizzate per emettere i certificati dei TSS sono generate e gestite, ivi incluso quanto riguarda la generazione e gestione dei relativi certificati, con modalità analoghe a quanto indicato al Capitolo 7 per le chiavi utilizzate per emettere i certificati qualificati, in termini di sicurezza di locali, di modalità di accesso ai sistemi, ecc. In particolare esibisce:
    a. le procedure di generazione delle chiavi e dei certificati della CA utilizzata per la TSA;
    b. i verbali di effettuazione delle procedure di cui al punto a;
    c. documentazione che dimostri che si sono utilizzati algoritmi e chiavi conformi con le norme vigenti.
2. Esibisce le procedure di generazione delle chiavi di firma dei TSS da cui emerga che esse sono generate in sicurezza sotto il controllo del relativo Responsabile.
3. Esibisce i verbali di esecuzione delle procedure di generazione delle chiavi di firma dei TSS di cui al punto 2.
4. Consente al verificatore l'accesso ai locali e ai sistemi dove sono gestiti i TSS e le relative CA, sotto la supervisione di proprio personale addetto e nel rispetto delle norme di sicurezza indicate nel Piano della Sicurezza.
5. Esibisce le procedure per il rilascio dei certificati ai TSS, ivi inclusa la richiesta di certificazione.
6. Esibisce tutti i certificati non scaduti rilasciati alle chiavi dei TSS.

10.2.3 Il valutatore

1. Verifica dalle procedure e dai verbali esibiti che le chiavi utilizzate per emettere i certificati dei TSS sono generate e gestite, ivi incluso quanto riguarda la generazione e gestione dei relativi certificati, con modalità analoghe a quelle previste per l'emissione dei certificati qualificati, in termini di sicurezza di locali, di modalità di accesso ai sistemi, ecc. come indicato al Capitolo 7.

2. Verifica che i certificati delle CA per le TSA si riferiscano a coppie di chiavi diverse da quelle utilizzate per la generazione dei certificati qualificati.
3. Verifica che ogni TSS utilizzi una propria coppia di chiavi di firma non condivisa con altri sistemi TSS e che nei relativi certificati, conformi con ISO/IEC 9594-8:2001, sia riportato l'identificativo del TSS.

   Nota: in particolari configurazioni in un sistema TSS possono essere presenti più TSU, ciascuno dei quali firma i TST. In questo caso è opportuno che ogni TSU abbia una propria coppia di chiavi di firma. Infatti una differente coppia di chiavi per ogni TSU consente un maggior controllo in caso di incidente di sicurezza. In ogni caso l'identificativo del TSS deve essere uguale per tutti i TSU afferenti al medesimo TSS.
4. Verifica che i certificati di TSS relativi alle marche temporali emesse dal certificatore siano conformi con i requisiti del Titolo III della Deliberazione CNIPA 4/2005.
5. Verifica che dai certificati di ogni TSU risulti che tra il notBefore di un certificato e quello del successivo non passi un tempo maggiore di quello previsto dall'art. 46.2 del DPCM 13/1/2004.
6. Verifica che nelle CRL non risultino certificati delle chiavi dei TSS revocati per motivi diversi da keyCompromise, cACompromise, affiliationChanged.

   Nota: un altro motivo accettabile è cessationOfOperation, ma è applicabile solo nel caso in cui l'ispezione riguardi un certificatore non più in esercizio come certificatore accreditato. La revoca, cioè, non deve dipendere dalla sostituzione della coppia di chiavi usata dal TSS interessato.

10.3 Dispositivi di firma delle CA per la TSA e di quelli per i TSS

Finalità: il certificatore garantisce la sicurezza dei dispositivi di firma per tutto il loro ciclo di vita e che le chiavi siano generate e gestite sotto adeguato controllo

10.3.1 Normativa

Non esiste una normativa specifica per i dispositivi di firma per la generazione di marche temporali o per le CA relative.

Ai primi si applica quanto previsto per i dispositivi di firma dei titolari (DPCM 13/1/2004 Art. 3.1: "*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.*").

Ai secondi si applica quanto previsto per le CA che emettono certificati qualificati (DPCM 13/1/2004 Art. 47.1: "*Alle chiavi di certificazione utilizzate, ai sensi dell'articolo 46, comma 3, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.*").

10.3.2 Il certificatore

1. Analogamente a quanto indicato al Capitolo 7, esibisce procedure e verbali che dimostrino che i dispositivi utilizzati per emettere i certificati dei TSS sono gestiti, anche per quanto riguarda le certificazione di sicurezza, con modalità analoghe a quelle previste per i dispositivi utilizzati per l'emissione dei certificati qualificati, in termini di sicurezza di locali, di modalità di accesso ai sistemi, ecc.
2. Esibisce documentazione da cui emerga che i dispositivi di firma dei TSS e le procedure per la loro gestione sono conformi ai requisiti previsti per i dispositivi di firma dei titolari;

10.3.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al capitolo 10.3.2.
2. Verifica che dalle procedure esibite risulti che della chiave privata dei TSS non sia fatta copia, anche ove il dispositivo lo consenta.

10.4 Formato e contenuto dei TST

Finalità: le marche temporali devono rispettare il formato previsto dalla normativa in vigore allo scopo di agevolare l'interoperabilità

10.4.1 Normativa

DPCM 13/1/2004

Art. 45. Informazioni contenute nella marca temporale.

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 4

Art. 8. Regole per i servizi di validazione temporale

10.4.2 Il certificatore

1. Fornisce al valutatore marche temporali preesistenti e altre di cui il valutatore può chiedere l'emissione appositamente per effettuare i controlli necessari.

10.4.3 Il valutatore

1. Verifica che le marche temporali siano conformi con quanto indicato all'art. 8 della Deliberazione CNIPA 4/2005.
2. Può chiedere l'emissione di marche temporali appositamente per effettuare i controlli necessari relativi al formato.

10.5 Algoritmi

Finalità: gli algoritmi che il certificatore utilizza direttamente, così come i programmi di verifica che esso fornisce ai propri titolari, devono essere conformi alla normativa.

10.5.1 Normativa

DPCM 13/1/2004

Art. 3. Norme tecniche di riferimento. – commi 1, 2

Art. 5. Generazione delle chiavi.

Art. 10. Verifica delle firme digitali.

Art. 30. Piano per la sicurezza. – comma 1, lettera f)

Art. 53. Norme transitorie. Commi 1, 2

Deliberazione CNIPA 4/2005

Art. 8. Regole per i servizi di validazione temporale – commi 2, 3

Circolare 6 settembre 2005, n. 48

… [omissis] alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

a) algoritmi di generazione e di verifica delle firme utilizzati e supportati dal certificatore;

b) algoritmi di hash utilizzati e supportati dal certificatore;

c) lunghezza delle chiavi;

10.5.2 Il certificatore

1. Esibisce documentazione che dimostri:
    a. l'adozione di algoritmi e chiavi conformi con quanto previsto nell'art. 53 del DPCM 13/1/2004, come da esso stesso indicato nel Piano per la sicurezza di cui all'art. 30 del medesimo DPCM e nella dichiarazione tecnica richiesta dalla Circolare CNIPA 48/2005;

        Nota: di questa documentazione fa parte la certificazione dei dispositivi di firma, integrata dalle procedure di generazione delle chiavi e delle firme in vigore presso il certificatore;

    b. la fornitura ai titolari di applicazioni di verifica delle marche temporali in grado di gestire gli algoritmi suddetti;
    c. che adeguata informativa è fornita ai titolari sulla necessità di utilizzare applicazioni di verifica delle marche temporali che utilizzino algoritmi e chiavi conformi a quanto indicato al punto a.

10.5.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 10.5.2, analoga a quella di cui al punto 1 del paragrafo 8.5.2.
2. Verifica che rispondano ai requisiti in vigore algoritmi e lunghezza delle chiavi utilizzati:
    a. dalle applicazioni fornite dal certificatore agli utenti che richiedono le marche temporali,
    b. dalle applicazioni utilizzate dal certificatore per emettere i certificati di marcatura temporale e per emettere le marche temporali.

10.6 Modalità per la richiesta dei TST

Finalità: assicurare che le richieste di marche temporali siano effettuate in modo sicuro e siano conformi con la normativa tecnica e giuridica in vigore.

10.6.1 Normativa

DPCM 13/1/2004

Art. 38. Manuale operativo. – comma 3, lettera r)

Art. 51. Richiesta di validazione temporale.

Deliberazione CNIPA 4/2005

Art. 8. Regole per i servizi di validazione temporale – comma 1

10.6.2 Il certificatore

1. Esibisce la procedura e il programma di richiesta dei TST forniti ai titolari, conformemente con quanto indicato nel Manuale operativo, da cui risulti il rispetto dell'art. 51 del DPCM 13/1/2004 e dell'art. 8 della Deliberazione CNIPA 4/2005.
2. Abilita il valutatore a richiedere marche temporali ai propri TSS, ove possibile anche più marche temporali per la stessa evidenza informatica.

10.6.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 10.6.2.
2. Può richiedere marche temporali emessi dai vari TSS del certificatore avvalendosi della procedura e del programma forniti dal certificatore ai titolari.
3. Verifica che il tempo intercorso tra il momento della ricezione della richiesta da parte dei TSS e l'ora riportata nella marca temporale non superi il minuto primo.

10.7 Gestione e operatività dei sistemi di TSA

Finalità: Applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute, tra cui gli standard di sicurezza emessi da organismi internazionali.

10.7.1 Normativa

La gestione e operatività della TSA sono analoghe a quanto indicato per la CA ai capitoli 9.1 – Gestione della sicurezza, 9.2 – Gestione degli asset, 9.3 – Gestione del personale, 9.4 – Sicurezza fisica, 9.5 – Altri aspetti della gestione operativa, 9.6 – Gestione accesso ai sistemi, 9.7 – Utilizzo e manutenzione dei sistemi del certificatore.

Le esigenze indicate al capitolo 9.8 – Business Continuity management differiscono da quelle della TSA in quanto non è possibile prevedere una copia delle chiavi di TSS da conservare presso il sito di disaster recovery in quanto una tale misura è prevista solo per le chiavi di CA.

Per quanto riguarda l'esigenza di continuità nel pubblicare le informazioni sullo stato dei certificati di TSS e l'Elenco dei certificatori accreditati vale quanto previsto per la CA.

10.7.2 Il certificatore

1. Esibisce documentazione (procedure, verbali, certificazioni, ecc) che dimostri l'aderenza delle misure prese dal certificatore al fine di assicurare alla TSA misure di sicurezza e organizzative analoghe a quelle della CA, come indicato al Capitolo 9.
2. Consente al valutatore di accedere ai locali e ai sistemi della TSA in conformità con le misure di sicurezza previste.
3. Esibisce evidenza che sono state prese misure onde assicurare il rispetto dei tempi di risposta indicati all'art. 51 comma 5 del DPCM 13/1/2004.

10.7.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al punto 1 del paragrafo 10.7.2.
2. Può accedere ai locali e ai sistemi della TSA.

Capitolo 11

Firme e documenti

11.1 Programmi di firma

Finalità: assicurare che i documenti da firmare siano presentati ai titolari chiaramente e senza ambiguità prima dell'apposizione della firma, e che essi confermino la volontà di generare la firma, fatto salvo quanto previsto dalla normativa per le procedure automatiche di firma.

Nota: la normativa non richiede né prevede che i certificatori forniscano ai titolari un'applicazione di firma, ma questa è ormai una prassi diffusa.

11.1.1 Normativa

Dlgs 82/2005

Art. 35. Dispositivi sicuri e procedure per la generazione della firma. – commi 2, 3

DPCM 13/1/2004

Art. 38. Manuale operativo. – comma 3, lettera t)

11.1.2 Il certificatore

1. Esibisce i programmi di firma che eventualmente distribuisce ai propri titolari e la relativa documentazione da cui emerga che ai titolari è possibile prendere visione del documento prima di firmarlo.
2. Esibisce, ove possibile, certificazione indipendente che attesti quanto sopra.
3. Esibisce i documenti di consegna dei programmi di cui sopra, sottoscritti dal titolare, con le relative eventuali istruzioni integrative di quanto indicato nel Manuale operativo.
4. Consente al valutatore l'uso dei programmi di firma.

11.1.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al paragrafo 11.1.2.
2. Verifica l'effettiva rispondenza dell'applicazione di firma ai principali requisiti di legge relativi all'obbligo di presentare al titolare i documenti informatici prima dell'apposizione della firma chiaramente e senza ambiguità e di richiedere conferma della volontà di generare la firma.

11.2 Formato firma

Finalità: informare i titolari del formato di firma avente validità legale in Italia.

11.2.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere e), l)

DPCM 13/1/2004

Art. 36. Formato della firma.

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 6

Art. 12. Busta crittografica di firma – commi da 1 a 9

Art. 13. Regole per l'apposizione di firme multiple

11.2.2 Il certificatore

1. Esibisce documentazione e procedure operative che dimostrino che esso include nella informativa fornita ai richiedenti dei certificati "su mezzi di comunicazione durevoli", come previsto all'art. 32.3, lettera l) del Dlgs 82/2005, anche una chiara indicazione sui formati di firma utilizzabili e sulla opportunità di acquisire ulteriori informazioni accedendo al sito www.cnipa.gov.it.
2. Ove il certificatore fornisca ai titolari alcuni client di firma essi devono soddisfare i requisiti relativi al formato di firma di cui alla normativa citata al paragrafo 11.2.1.

11.2.3 Il valutatore

1. Verifica l'esistenza della documentazione di cui al punto 1 del paragrafo 11.2.2.
2. Ove il certificatore fornisca ai titolari uno o più client di firma, verifica che essi rispondano ai requisiti relativi al formato di firma di cui alla normativa citata al paragrafo 11.2.1.

11.3 Verifica firma

Finalità: fornire ai titolari uno o più client di verifica delle firme interoperabili con i documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative.

11.3.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere e), l)

DPCM 13/1/2004

Art. 10. Verifica delle firme digitali.

Art. 36. Formato della firma.

Art. 38. Manuale operativo. – comma 3, lettera s)

Art. 40. Obblighi per i certificatori accreditati. – comma 2

Deliberazione CNIPA 4/2005

Art. 2. Ambito di applicazione e contenuto – comma 7

Art. 12. Busta crittografica di firma – commi da 1 a 9

Art. 13. Regole per l'apposizione di firme multiple

Art. 14. Requisiti delle applicazioni di verifica

Art. 15. Operatività – comma 6

11.3.2 Il certificatore

1. Esibisce i client di verifica delle firme che esso fornisce ai titolari.
2. Esibisce le istruzioni relative al client di verifica delle firme da cui risulti la rispondenza ai requisiti di legge.

11.3.3 Il valutatore

1. Verifica che i client di verifica delle firme di cui all'art. 10 del DPCM 13/1/2004:
    a. siano conformi con quanto indicato all'art. 14 della Deliberazione CNIPA 4/2005;
    b. siano interoperabili con i documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative, come previsto dall'art. 40 comma 2 del DPCM 13/1/2004. Un esempio di tale documento è l'Elenco pubblico dei certificatori.

11.4 Formato documenti

Finalità: fornire ai titolari indicazioni sulle caratteristiche di immutabilità dei documenti da firmare.

11.4.1 Normativa

Dlgs 82/2005

Art. 32. Obblighi del titolare e del certificatore. – comma 3, lettere e), l)

DPCM 13/1/2004

Art. 3. Norme tecniche di riferimento. – comma 3

Art. 42. Rappresentazione del documento informatico.

11.4.2 Il certificatore

1. Esibisce eventuale documentazione, fornita ai titolari in aggiunta al Manuale operativo, che indichi i formati dei documenti utilizzabili e le modalità operative a cui il titolare deve attenersi per operare nel rispetto della normativa.

11.4.3 Il valutatore

1. Verifica che nel Manuale operativo sia indicato quanto richiesto all'art. 42 del DPCM 13/1/2004.
2. Verifica che l'eventuale documentazione di cui al paragrafo 11.4.2 non sia in contrasto con quanto indicato nel Manuale operativo.

Capitolo 12

Auditing

Finalità: verificare, tramite ispezioni programmate e non, il rispetto dei requisiti tecnici e di legge che governano l'attività del certificatore.

12.1 Normativa

DPCM 13/1/2004

Art. 33. Organizzazione del personale del certificatore. – comma 1, lettera l)

Nota: misure relative all'auditing sono indicate nello standard ISO/IEC 17799: 2005.

12.2 Il certificatore

1. Esibisce piani e procedure che dimostrino l'esecuzione periodica e anche estemporanea di ispezioni, effettuate per verificare il rispetto delle procedure, da parte:
   a. di personale interno ai singoli reparti;
   b. di personale del reparto aziendale preposto ai controlli di qualità e/o all'audit;
   c. di enti esterni.
2. Esibisce verbali delle ispezioni da cui risultino la loro effettuazione regolare, o anche estemporanea ove necessario, le risultanze, le raccomandazioni. A fronte di eccezioni e raccomandazioni sollevate dagli ispettori esibisce al valutatore le azioni intraprese per ovviarvi.
3. Esibisce documentazione dalla quale risulti che gli strumenti adoperati dagli ispettori per effettuare le verifiche sono protetti da accessi non autorizzati onde evitarne manomissioni.
4. Consente al valutatore di effettuare controlli e verifiche.

12.3 Il valutatore

1. Verifica l'esistenza di piani di ispezione che prevedano, e di verbali che confermino, l'effettuazione di ispezioni regolari, o anche estemporanee ove necessario.
2. Verifica che le eccezioni sollevate dagli ispettori siano state adeguatamente prese in considerazione.
3. Verifica che gli strumenti utilizzati ai fini delle verifiche di auditing siano protetti da accessi non autorizzati.
4. Può richiedere di effettuare controlli e verifiche sugli strumenti utilizzati dagli auditor o dagli ispettori interni onde verificare se non risultino macroscopiche violazioni alle procedure previste per proteggerli da accessi non autorizzati onde evitare manomissioni.

Capitolo 13

Normativa Europea sulla firma elettronica

13.1 Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche.5

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare gli articoli 47, paragrafo 2, 55 e 95,

vista la proposta della Commissione[6],

visto il parere del Comitato economico e sociale[7],

visto il parere del Comitato delle regioni[8],

deliberando secondo la procedura di cui all'articolo 251 del trattato[9],

considerando quanto segue:

(1) il 16 aprile 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni una comunicazione relativa ad un'iniziativa europea in materia di commercio elettronico;

(2) l'8 ottobre 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni una comunicazione intitolata "Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche - Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura";

(3) il 10 dicembre 1997 il Consiglio ha invitato la Commissione a presentare quanto prima una proposta di direttiva del Parlamento europeo e del Consiglio relativa alle firme digitali;

(4) le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati; la divergenza delle norme in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico; invece, un quadro comunitario chiaro relativo alle condizioni che si applicano alle firme elettroniche rafforzerà la fiducia nelle nuove tecnologie e la loro accettazione generale; la normativa negli Stati membri non dovrebbe essere di ostacolo alla libera circolazione di beni e di servizi nel mercato interno;

---

[5] (incluse le rettifiche introdotte dalla Gazzetta Ufficiale delle Comunità europee L 119/4 del 7 maggio 2002).

[6] GU C 325 del 23.10.1998, pag. 5.

[7] GU C 40 del 15.2.1999, pag. 29.

[8] GU C 93 del 6.4.1999, pag. 33.

[9] Parere del Parlamento europeo del 13 gennaio 1999 (GU C 104 del 14.4.1999, pag. 49), posizione comune del Consiglio del 28 giugno 1999 (GU C 243 del 27.8.1999, pag. 33) e decisione del Parlamento europeo del 27 ottobre 1999 (non ancora pubblicata nella Gazzetta ufficiale). Decisione del Consiglio del 30 novembre 1999.

(5) occorrerebbe promuovere l'interoperabilità dei prodotti di firma elettronica; a norma dell'articolo 14 del trattato, il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci; per garantire la libera circolazione nell'ambito del mercato interno e infondere fiducia nelle firme elettroniche, è necessaria la conformità ai requisiti essenziali specifici relativi ai prodotti di firma elettronica, fatti salvi il regolamento (CE) n. 3381/94 del Consiglio, del 19 dicembre 1994, che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso[10], e la decisione 94/942/PESC del Consiglio del 19 dicembre 1994, relativa all'azione comune adottata dal Consiglio riguardante il controllo delle esportazioni di beni a duplice uso[11];

(6) la presente direttiva non armonizza la fornitura di servizi rispetto al carattere riservato dell'informazione quando sono oggetto di disposizioni nazionali inerenti all'ordine pubblico o alla pubblica sicurezza;

(7) il mercato interno consente anche la libera circolazione delle persone la quale si traduce in una maggiore necessità, per i cittadini dell'Unione europea e per le persone che vi risiedono, di trattare con le autorità di Stati membri diversi da quello in cui risiedono; la disponibilità di comunicazioni elettroniche potrebbe essere di grande aiuto a questo riguardo;

(8) la rapida evoluzione tecnologica e il carattere globale di Internet rendono necessario un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico;

(9) le firme elettroniche verranno usate in svariate circostanze ed applicazioni, che comporteranno un'ampia gamma di nuovi servizi e prodotti facenti uso di firme elettroniche o ad esse collegati; la definizione di tali prodotti e servizi non dovrebbe essere limitata al rilascio e alla gestione di certificati, ma comprenderebbe anche ogni altro servizio e prodotto facente uso di firme elettroniche, o ad esse ausiliario, quali servizi di immatricolazione, servizi di apposizione del giorno e dell'ora, servizi di repertorizzazione, servizi informatici o di consulenza relativi alle firme elettroniche;

(10) il mercato interno consente ai prestatori di servizi di certificazione di sviluppare le proprie attività transfrontaliere ai fini di accrescere la competitività e, pertanto, di offrire ai consumatori e alle imprese nuove opportunità di scambiare informazioni e di effettuare negozi per via elettronica in modo sicuro, indipendentemente dalle frontiere; al fine di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte, i prestatori di servizi di certificazione dovrebbero essere liberi di fornire i rispettivi servizi senza preventiva autorizzazione; per autorizzazione preventiva non si intende soltanto qualsiasi permesso che il prestatore di servizi interessato deve ottenere dalle autorità nazionali prima di poter fornire i propri servizi di certificazione, ma anche ogni altra misura avente effetto equivalente;

(11) i sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito possono offrire ai prestatori di servizi di certificazione il quadro appropriato per l'ulteriore sviluppo dei loro servizi verso i livelli di fiducia, sicurezza e qualità richiesti dall'evoluzione del mercato; tali sistemi dovrebbero incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; questi ultimi dovrebbero essere liberi di aderire a tali sistemi di accreditamento e di trarne vantaggio;

(12) i servizi di certificazione possono essere forniti o da un'entità pubblica ovvero da una persona giuridica o fisica quando è costituita secondo il diritto nazionale; gli Stati membri non dovrebbero vietare ai prestatori di servizi di certificazione di operare al di fuori dei sistemi di accreditamento facoltativo; si dovrebbe garantire che tali sistemi di accreditamento non riducano la concorrenza nel settore dei servizi di certificazione;

(13) gli Stati membri possono decidere come garantire il controllo del rispetto delle disposizioni contenute nella presente direttiva; quest'ultima non esclude l'istituzione di sistemi di controllo basati sul settore privato; la presente direttiva non obbliga i prestatori di servizi di certificazione a chiedere il controllo in base a un qualsiasi sistema d'accreditamento applicabile;

(14) è importante raggiungere l'equilibrio tra le esigenze dei consumatori e le esigenze delle imprese;

[10] GU L 367 del 31.12.1994, pag. 1. Regolamento modificato dal regolamento (CE) n. 837/95 (GU L 90 del 21.4.1995, pag. 1).

[11] GU L 367 del 31.12.1994, pag. 8. Decisione modificata da ultimo dalla decisione 1999/193/PESC (GU L 73 del 19.3.1999, pag. 1).

(15) considerando che l'allegato III prevede requisiti relativi a dispositivi per la creazione di una firma sicura al fine di assicurare la funzionalità delle firme elettroniche avanzate; esso non contempla la globalità dell'ambiente del sistema in cui tali dispositivi operano; il funzionamento del mercato interno impone alla Commissione e agli Stati membri un'azione rapida al fine di permettere la designazione degli organismi preposti alla valutazione della conformità dei dispositivi di firma sicura rispetto all'allegato III; per rispondere alle esigenze del mercato, la valutazione della conformità deve essere tempestiva ed efficiente;

(16) la presente direttiva contribuisce all'uso e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità; le firme elettroniche usate esclusivamente all'interno di sistemi basati su accordi volontari di diritto privato fra un numero determinato di partecipanti non esigono una disciplina legislativa comune; nella misura consentita dal diritto nazionale, andrebbe rispettata la libertà delle parti di accordarsi sulle condizioni di accettazione dei dati firmati in modo elettronico; alle firme elettroniche utilizzate in tali sistemi non dovrebbero essere negate l'efficacia giuridica e l'ammissibilità come mezzo probatorio nei procedimenti giudiziari;

(17) la presente direttiva non è diretta ad armonizzare le normative nazionali sui contratti, in particolare in materia di conclusione ed esecuzione dei contratti, od altre formalità di natura extracontrattuale concernenti l'apposizione di firme; per tale motivo, le disposizioni sugli effetti giuridici delle firme elettroniche non dovrebbero pregiudicare i requisiti formali previsti dal diritto nazionale sulla conclusione dei contratti o le regole di determinazione del luogo della conclusione del contratto;

(18) la registrazione e la copia di dati per la creazione di una firma potrebbero costituire una minaccia per la validità giuridica delle firme elettroniche;

(19) le firme elettroniche saranno utilizzate nel settore pubblico nell'ambito delle amministrazioni nazionali e comunitarie e nelle comunicazioni tra tali amministrazioni nonché con i cittadini e gli operatori economici, ad esempio nei settori degli appalti pubblici, della fiscalità, della previdenza sociale, della sanità e dell'amministrazione della giustizia;

(20) criteri armonizzati relativi agli effetti giuridici delle firme elettroniche manterranno un quadro giuridico coerente in tutta la Comunità; il diritto nazionale stabilisce differenti requisiti per la validità giuridica delle firme autografe; i certificati possono essere usati per confermare l'identità di una persona che ricorre alla firma elettronica; le firme elettroniche avanzate basate su un certificato qualificato mirano ad un più alto livello di sicurezza; le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura possono essere considerate giuridicamente equivalenti alle firme autografe solo se sono rispettati i requisiti per le firme autografe;

(21) al fine di contribuire all'accettazione generale dei metodi di autenticazione elettronici, è necessario garantire che le firme elettroniche possano essere utilizzate come prove nei procedimenti giudiziari in tutti gli Stati membri; il riconoscimento giuridico delle firme elettroniche dovrebbe basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione rilasciata al prestatore di servizi di certificazione interessato; il diritto nazionale disciplina la definizione dei campi giuridici in cui possono essere impiegati documenti elettronici e firme elettroniche; la presente direttiva lascia impregiudicata la facoltà degli organi giurisdizionali nazionali di deliberare in merito alla conformità rispetto ai requisiti della presente direttiva e non lede le norme nazionali in materia di libero uso delle prove in giudizio;

(22) la responsabilità dei prestatori di servizi di certificazione che forniscono tali servizi al pubblico è disciplinata dal diritto nazionale;

(23) lo sviluppo del commercio elettronico internazionale rende necessarie soluzioni transfrontaliere che coinvolgano i paesi terzi; al fine di assicurare l'interoperabilità a livello globale, potrebbero essere utili accordi su regole multilaterali con paesi terzi concernenti il riconoscimento reciproco dei servizi di certificazione;

(24) al fine di accrescere la fiducia da parte degli utenti nelle comunicazioni elettroniche e nel commercio elettronico, i prestatori di servizi di certificazione devono osservare la legislazione in materia di protezione dei dati e la vita privata degli individui;

(25) le disposizioni sull'uso degli pseudonimi nei certificati non dovrebbe impedire agli Stati membri di chiedere l'identificazione delle persone in base alla normativa comunitaria o alla legislazione nazionale;

(26) le misure necessarie per l'attuazione della presente direttiva devono essere adottate ai sensi dell'articolo 2 della decisione 1999/468/CE del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione[12];

(27) due anni dopo la sua attuazione la Commissione presenterà una relazione su questa direttiva al fine di garantire tra l'altro che il progresso tecnologico o il mutamento del quadro giuridico non abbiano creato ostacoli al raggiungimento degli obiettivi sanciti nella stessa; la Commissione dovrebbe esaminare le implicazioni dei settori tecnici connessi e presentare una relazione al riguardo al Parlamento europeo e al Consiglio;

(28) secondo i principi di sussidiarietà e proporzionalità di cui all'articolo 5 del trattato, l'obiettivo della creazione di un quadro giuridico armonizzato per la fornitura di firme elettroniche e dei servizi relativi non può essere sufficientemente realizzato dagli Stati membri e può dunque essere realizzato meglio a livello comunitario; la presente direttiva non va al di là di quanto necessario per il raggiungimento degli obiettivi del trattato,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1.

Ambito di applicazione.

La presente direttiva è volta ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico. Essa istituisce un quadro giuridico per le firme elettroniche e taluni servizi di certificazione al fine di garantire il corretto funzionamento del mercato interno.

Essa non disciplina aspetti relativi alla conclusione e alla validità dei contratti o altri obblighi giuridici quando esistono requisiti relativi alla forma prescritti dal diritto nazionale o comunitario, né pregiudica le norme e i limiti che disciplinano l'uso dei documenti contenuti nel diritto nazionale o comunitario.

Articolo 2.

Definizioni.

Ai fini della presente direttiva, valgono le seguenti definizioni:

1) "firma elettronica", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;

2) "firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:

a) essere connessa in maniera unica al firmatario;

b) essere idonea ad identificare il firmatario;

c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;

d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;

3) "firmatario", una persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;

4) "dati per la creazione di una firma", dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;

5) "dispositivo per la creazione di una firma", un software configurato o un hardware usato per applicare i dati per la creazione di una firma;

[12] GU L 184 del 17.7.1999, pag. 23.

6) "dispositivo per la creazione di una firma sicura"[13], un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'allegato III;

7) "dati per la verifica della firma", dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;

8) "dispositivo di verifica della firma", un software configurato o un hardware usato per applicare i dati di verifica della firma;

9) "certificato", un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona;

10) "certificato qualificato", un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;

11) "prestatore di servizi di certificazione", un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;

12) "prodotto di firma elettronica", hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche;

13) "accreditamento facoltativo", qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo.

Articolo 3.

Accesso al mercato.

1. Gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione.

2. Fatto salvo il paragrafo 1, gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi volti a fornire servizi di certificazione di livello più elevato. Tutte le condizioni relative a tali sistemi devono essere obiettive, trasparenti, proporzionate e non discriminatorie. Gli Stati membri non possono limitare il numero di prestatori di servizi di certificazione accreditati per motivi che rientrano nell'ambito di applicazione della presente direttiva.

3. Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilasci al pubblico certificati qualificati.

4. La conformità dei dispositivi per la creazione di una firma sicura ai requisiti di cui all'allegato III è determinata dai pertinenti organismi pubblici o privati designati dagli Stati membri. Secondo la procedura di cui all'articolo 9 la Commissione fissa i criteri in base ai quali gli Stati membri stabiliscono se un organismo può essere designato.

La conformità ai requisiti di cui all'allegato III accertata dagli organismi di cui al primo comma è riconosciuta da tutti gli Stati membri.

5. Secondo la procedura di cui all'articolo 9 la Commissione può determinare e pubblicare nella Gazzetta ufficiale delle Comunità europee i numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica. Un prodotto di firma elettronica conforme a tali norme viene considerato dagli Stati membri conforme ai requisiti di cui all'allegato II, lettera f) e all'allegato III.

[13] La dizione "dispositivo di firma sicura" deriva da un'errata traduzione dall'inglese: la versione corretta è "dispositivo sicuro di firma". Questo errore ricorre più volte nel testo della Direttiva.

6. Gli Stati membri e la Commissione cooperano per promuovere lo sviluppo e l'uso dei dispositivi di verifica della firma, alla luce delle raccomandazioni per la verifica della firma sicura di cui all'allegato IV e nell'interesse dei consumatori.

7. Gli Stati membri possono assoggettare l'uso delle firme elettroniche nel settore pubblico ad eventuali requisiti supplementari. Tali requisiti debbono essere obiettivi, trasparenti, proporzionati e non discriminatori e riguardare unicamente le caratteristiche specifiche dell'uso di cui trattasi. Tali requisiti non possono rappresentare un ostacolo ai servizi transfrontalieri per i cittadini.

Articolo 4.

Principi del mercato interno.

1. Ciascuno Stato membro applica le disposizioni nazionali da esso adottate in base alla presente direttiva ai prestatori di servizi di certificazione stabiliti nel suo territorio e ai servizi da essi forniti. Gli Stati membri non possono limitare la prestazione di servizi di certificazione originati in un altro Stato membro nella materia disciplinata dalla presente direttiva.

2. Gli Stati membri consentono ai prodotti di firma elettronica conformi alla presente direttiva di circolare liberamente nel mercato interno.

Articolo 5.

Effetti giuridici delle firme elettroniche.

1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:

a) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e

b) siano ammesse come prova in giudizio.

2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:

- in forma elettronica, o

- non basata su un certificato qualificato, o

- non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero

- non creata da un dispositivo per la creazione di una firma sicura.

Articolo 6.

Responsabilità.

1. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico tale certificato, sia responsabile per danni provocati a entità o persone fisiche o giuridiche che facciano ragionevole affidamento su detto certificato:

a) per quanto riguarda l'esattezza di tutte le informazioni contenute nel certificato qualificato al momento del rilascio e il fatto che esso contenga tutti i dati prescritti per un certificato qualificato,

b) per la garanzia che, al momento del rilascio del certificato, il firmatario identificato nel certificato qualificato detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato,

c) la garanzia che i dati per la creazione della firma e i dati per la verifica della firma possano essere usati in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi entrambi,

a meno che il prestatore di servizi di certificazione provi di aver agito senza negligenza.

2. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato sia responsabile, nei confronti di entità o di persone fisiche o giuridiche che facciano ragionevole affidamento sul certificato, dei danni provocati, per la mancata registrazione della revoca del certificato, a meno che provi di aver agito senza negligenza.

3. Gli Stati membri provvedono a che un prestatore di servizi di certificazione possa indicare, in un certificato qualificato, i limiti d'uso di detto certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione deve essere esentato dalla responsabilità per i danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti nello stesso.

4. Gli Stati membri provvedono affinché un prestatore di servizi di certificazione abbia la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato, purché tali limiti siano riconoscibili da parte dei terzi.

Il prestatore di servizi di certificazione non è responsabile dei danni risultanti dal superamento di detto limite massimo.

5. I paragrafi da 1 a 4 lasciano impregiudicata la direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori[14].

Articolo 7.

Aspetti internazionali.

1. Gli Stati membri provvedono a che i certificati rilasciati al pubblico come certificati qualificati da un prestatore di servizi di certificazione stabilito in un paese terzo siano riconosciuti giuridicamente equivalenti ai certificati rilasciati da un prestatore di servizi di certificazione stabilito nella Comunità, in presenza di una delle seguenti condizioni:

a) il prestatore di servizi di certificazione possiede i requisiti di cui alla presente direttiva e sia stato accreditato in virtù di un sistema di accreditamento facoltativo stabilito in uno Stato membro, oppure

b) il certificato è garantito da un prestatore di servizi di certificazione stabilito nella Comunità, in possesso dei requisiti di cui alla presente direttiva, oppure

c) il certificato o il prestatore di servizi di certificazione è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e paesi terzi o organizzazioni internazionali.

2. Al fine di agevolare servizi di certificazione transfrontalieri con paesi terzi e il riconoscimento giuridico delle firme elettroniche avanzate che hanno origine in paesi terzi, la Commissione presenta, se del caso, proposte miranti all'effettiva attuazione di norme e di accordi internazionali applicabili ai servizi di certificazione. In particolare, ove necessario, essa presenta al Consiglio proposte relative a mandati per la negoziazione di accordi bilaterali e multilaterali con paesi terzi e organizzazioni internazionali. Il Consiglio decide a maggioranza qualificata.

3. Ogniqualvolta la Commissione è informata di difficoltà che le imprese comunitarie incontrano riguardo all'accesso al mercato di paesi terzi, essa può, se necessario, presentare al Consiglio proposte in merito a un appropriato mandato di negoziato per ottenere diritti paragonabili per le imprese comunitarie in tali paesi terzi. Il Consiglio decide a maggioranza qualificata.

Le misure adottate a norma di questo paragrafo lasciano impregiudicati gli obblighi della Comunità e degli Stati membri derivanti da accordi internazionali in materia.

Articolo 8.

Protezione dei dati.

[14] GU L 95 del 21.4.1993, pag. 29.

1. Gli Stati membri provvedono a che i prestatori di servizi di certificazione e gli organismi nazionali responsabili dell'accreditamento o della supervisione si conformino alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[15].

2. Gli Stati membri consentono a un prestatore di servizi di certificazione che rilascia certificati al pubblico di raccogliere dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

3. Fatti salvi gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi, gli Stati membri non vietano al prestatore di servizi di certificazione di riportare sul certificato uno pseudonimo in luogo del nome del firmatario.

Articolo 9.

Comitato.

1. La Commissione è assistita da un "comitato per la firma elettronica", in prosieguo denominato "il comitato".

2. Nei casi in cui si fa riferimento al presente paragrafo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE, tenuto conto dell'articolo 8 della stessa.

Il periodo di cui all'articolo 4, paragrafo 3 della decisione 1999/468/CE è fissato a tre mesi.

3. Il comitato adotta il proprio regolamento interno.

Articolo 10.

Compiti del comitato.

Il comitato precisa i requisiti di cui agli allegati della presente direttiva, i criteri di cui all'articolo 3, paragrafo 4 e le norme generalmente riconosciute per i prodotti di firma elettronica istituite e pubblicate a norma dell'articolo 3, paragrafo 5, secondo la procedura di cui all'articolo 9, paragrafo 2.

Articolo 11.

Notificazione.

1. Gli Stati membri comunicano alla Commissione e agli altri Stati membri le seguenti informazioni:

a) sistemi di accreditamento facoltativi nazionali ed ogni requisito supplementare a norma dell'articolo 3, paragrafo 7;

b) nomi e indirizzi degli organismi nazionali responsabili dell'accreditamento e della supervisione nonché degli organismi di cui all'articolo 3, paragrafo 4;

c) i nomi e gli indirizzi di tutti i prestatori di servizi di certificazione nazionali accreditati.

2. Le informazioni di cui al paragrafo 1 e le loro eventuali variazioni sono notificate agli Stati membri al più presto.

Articolo 12.

Riesame.

1. Entro il 19 luglio 2003 la Commissione riesamina l'applicazione della presente direttiva e presenta una relazione in merito al Parlamento europeo e al Consiglio.

[15] GU L 281 del 23.11.1995, pag. 31.

2. Nel riesame si valuta, tra l'altro, se l'ambito di applicazione della presente direttiva debba essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. La relazione include in particolare una valutazione, sulla base dell'esperienza acquisita, degli aspetti relativi all'armonizzazione. La relazione è corredata, se del caso, di proposte legislative.

Articolo 13.

Attuazione.

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva anteriormente al 19 luglio 2001. Essi ne informano immediatamente la Commissione.

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle principali disposizioni di diritto interno che adottano nella materia disciplinata dalla presente direttiva.

Articolo 14.

Entrata in vigore.

La presente direttiva entra in vigore il giorno della pubblicazione nella Gazzetta ufficiale delle Comunità europee.

Articolo 15.

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

ALLEGATO I

Requisiti relativi ai certificati qualificati

I certificati qualificati devono includere:

a) l'indicazione che il certificato rilasciato è un certificato qualificato;

b) l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;

c) il nome del firmatario del certificato o uno pseudonimo identificato come tale;

d) l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;

e) i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;

f) un'indicazione dell'inizio e del termine del periodo di validità del certificato;

g) il codice d'identificazione del certificato;

h) la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;

i) i limiti d'uso del certificato, ove applicabili; e

j) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

ALLEGATO II

Requisiti relativi ai prestatori di servizi di certificazione che rilasciano certificati qualificati

I prestatori di servizi di certificazione devono:

a) dimostrare l'affidabilità necessaria per fornire servizi di certificazione;

b) assicurare il funzionamento di un servizio di repertorizzazione puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;

c) assicurare che la data e l'ora di rilascio o di revoca di un certificato possano essere determinate con precisione;

d) verificare con mezzi appropriati, secondo la legislazione nazionale l'identità e, eventualmente, le specifiche caratteristiche della persona cui è rilasciato un certificato qualificato;

e) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute;

f) utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;

g) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza nel corso della generazione di tali dati;

h) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla direttiva, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione;

i) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un adeguato periodo di tempo, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;

j) non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave;

k) prima di avviare una relazione contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

l) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:

- soltanto le persone autorizzate possano effettuare inserimenti e modifiche;

- l'autenticità delle informazioni sia verificabile,

- i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato,

- l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

ALLEGATO III

Requisiti relativi ai dispositivi per la creazione di una firma sicura

1. I dispositivi per la creazione di una firma sicura, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che:

a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è ragionevolmente garantita la loro riservatezza;

b) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro limiti ragionevoli di sicurezza, essere derivati e la firma è protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile;

c) i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi sicuri per la creazione di una firma non devono alterare i dati da firmare né impediscono che tali dati siano presentati al firmatario prima dell'operazione di firma.

ALLEGATO IV

Raccomandazioni per la verifica della firma sicura

Durante il processo relativo alla verifica della firma occorre garantire, entro limiti ragionevoli di certezza, che:

a) i dati utilizzati per la verifica della firma corrispondono ai dati comunicati al verificatore;

b) la firma è verificata in modo affidabile e i risultati della verifica correttamente comunicati;

c) il verificatore può, all'occorrenza, stabilire in modo attendibile i contenuti dei dati firmati;

d) l'autenticità e la validità del certificato necessario al momento della verifica della firma sono verificate in modo attendibile;

e) i risultati della verifica e dell'identità del firmatario sono comunicati correttamente;

f) l'uso di uno pseudonimo è chiaramente indicato;

g) qualsiasi modifica che incida sulla sicurezza può essere individuata.

13.2 Decisione della Commissione del 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.

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (1), in particolare l'articolo 3, paragrafo 5,

considerando quanto segue:

(1) L'allegato II, lettera f) e l'allegato III della direttiva 1999/ 93/CE fissano i requisiti dei prodotti di firma elettronica sicuri.

(2) Le specifiche tecniche necessarie per la produzione e la commercializzazione di prodotti basati sullo stato dell'arte tecnologico sono elaborate da organismi competenti in materia di normalizzazione.

(3) Il CEN (Comitato europeo di normalizzazione) e l'ETSI (Istituto europeo per le norme di telecomunicazioni) offrono, nell'ambito dell'EESSI (*European Electronic Signature Standardisation initiative*), una piattaforma europea aperta, partecipativa e flessibile per la ricerca di una posizione di consenso attorno allo sviluppo della Società dell'informazione in Europa. Tali organismi hanno sviluppato norme relative a prodotti di firma elettronica (*CWA-CEN workshop agreement* o *ETSI TS-ETSI technical specification*) fondate sui requisiti stabiliti dagli allegati della direttiva 1999/93/CE.

(4) Le misure stabilite nella presente decisione sono conformi al parere del comitato per la firma elettronica,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1.

I numeri di riferimento delle norme generalmente riconosciute relative a prodotti di firma elettronica figurano nell'allegato.

Articolo 2.

La Commissione procede ad un riesame del funzionamento della presente decisione entro due anni dalla data della sua pubblicazione nella Gazzetta ufficiale dell'Unione europea e riferisce al riguardo al comitato istituito ai sensi dell'articolo 9 paragrafo 1 della direttiva 1999/93/CE.

Articolo 3.

Gli Stati membri sono destinatari della presente decisione.

ALLEGATO

A. Elenco delle norme generalmente riconosciute relative ai prodotti di firma elettronica che vengono considerati dagli Stati membri conformi ai requisiti di cui all'allegato II, lettera f) della direttiva 1999/93/CE

— CWA 14167-1 (marzo 2003): *security requirements for trustworthy systems managing certificates for electronic signatures* — Part 1: *System Security Requirements*

— CWA 14167-2 (marzo 2002): *security requirements for trustworthy systems managing certificates for electronic signatures* — Part 2: *cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)*

B. Elenco delle norme generalmente riconosciute relative ai prodotti di firma elettronica che vengono considerati dagli Stati membri conformi ai requisiti di cui all'allegato III della direttiva 1999/93/CE

— CWA 14169 (marzo 2002): *secure signature-creation devices*

Capitolo 14

Norme Italiane sulla firma elettronica

14.1 Estratto dal Decreto legislativo 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale, come modificato dal Decreto legislativo 4 aprile 2006, n. 159

Capo I

PRINCIPI GENERALI

Sezione I

Definizioni, finalità e ambito di applicazione

Art. 1. Definizioni.

1. Ai fini del presente codice si intende per:

b) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

i) 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;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

r) firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente

modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare 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;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) 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.

Capo II

DOCUMENTO INFORMATICO E FIRME ELETTRONICHE; PAGAMENTI, LIBRI E SCRITTURE

Sezione I – Documento informatico

Art. 20. Documento informatico.

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo sicuro di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Art. 21. Valore probatorio del documento informatico sottoscritto.

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità**,** sicurezza, integrità e immodificabilità.

2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso 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.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

Art. 22. Documenti informatici originali e copie. Formazione e conservazione.

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 copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite ai sensi dell'articolo 71, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentito il Garante per la protezione dei dati personali.

Art. 23. Copie di atti e documenti informatici.

1. All'articolo 2712 del codice civile dopo le parole:

«riproduzioni fotografiche» è inserita la seguente:

«, informatiche».[16]

[16] Pertanto l'articolo 2712 del codice civile "Riproduzioni meccaniche" diventerà: "Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fotografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime".

2. 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 vigenti regole tecniche.

2-bis. Le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

3. 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, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

4. Le copie su supporto informatico di documenti originali non unici 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 assicurata dal responsabile della conservazione mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.

5. Le copie su supporto informatico di documenti, originali unici, 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 stabilite ai sensi dell'articolo 71.

6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Sezione II - Firme elettroniche e certificatori

Art. 24. Firma digitale

1. 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.

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

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Art. 25. Firma autenticata.

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.

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 23, comma 5.

Art. 26. Certificatori.

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.

2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.

3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

Art. 27. Certificatori qualificati.

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.

2. I certificatori di cui al comma 1, devono inoltre:

a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

4. Il CNIPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

Art. 28. Certificati qualificati.

1. I certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;

b) numero di serie o altro codice identificativo del certificato;

c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;

d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;

f) indicazione del termine iniziale e finale del periodo di validità del certificato;

g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.

3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3.

c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.

Art. 29. Accreditamento.

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.

2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.

3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:

a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;

b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti

che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.

4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.

8. Sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 30. Responsabilità del certificatore.

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;

b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;

c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;

d) sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.

3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Art. 31. Vigilanza sull'attività di certificazione.

1. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e accreditati.

Art. 32. Obblighi del titolare e del certificatore.

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:

a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;

b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle regole tecniche di cui all'articolo 71;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

f) non rendersi depositario di dati per la creazione della firma del titolare;

g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Art. 33. Uso di pseudonimi.

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale.

Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.

Art. 34. Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati.

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.

3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.

4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.

5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

Art. 35. Dispositivi sicuri e procedure per la generazione della firma.

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

a) sia riservata;

b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;

c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. L'apposizione di firme con procedura automatica è valida se l'attivazione della procedura medesima è chiaramente riconducibile alla volontà del titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente.

4. 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 di cui al comma 5.

5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Lo schema nazionale la cui attuazione non deve determinare nuovi o maggiori oneri per il bilancio dello Stato ed individua l'organismo pubblico incaricato di accreditare i centri di valutazione e di certificare le valutazioni di sicurezza. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

6. La conformità ai requisiti di sicurezza dei dispositivi sicuri per la creazione di una firma qualificata a quanto prescritto dall'allegato III della direttiva 1999/93/CE è inoltre riconosciuta se certificata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva stessa.

Art. 36. Revoca e sospensione dei certificati qualificati.

1. Il certificato qualificato deve essere a cura del certificatore:

a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;

b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;

d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.

3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 71.

Art. 37. Cessazione dell'attività.

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al CNIPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.

2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.

3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.

4. Il CNIPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.

14.2 Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

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'art. 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'art. 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 nella 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 22 giugno 1998, del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE del 20 luglio 1998, CE del Parlamento europeo e del Consiglio, 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'art. 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'art. 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'art. 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'art. 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'art. 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'art. 29-sexies del testo unico e all'art. 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'art. 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'art. 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. f) piano per la sicurezza contenuto in busta sigillata;

g. manuale operativo di cui al successivo art. 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'art. 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'art. 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'art. 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'art. 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'art. 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'art. 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.

Art. 17. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione.

1. La revoca del certificato qualificato relativo a chiavi di sottoscrizione viene effettuata dal certificatore mediante l'inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL/CSL).

2. Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione dell'aggiornamento della lista di revoca.

3. La revoca dei certificati è annotata nel giornale di controllo con la specificazione della data e dell'ora della pubblicazione della nuova lista.

Art. 18. Revoca su iniziativa del certificatore.

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

Art. 19. Revoca su richiesta del titolare.

1. La richiesta di revoca deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua decorrenza.

2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo di cui al successivo art. 38.

3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste al comma 2.

4. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 20. Revoca su richiesta del terzo interessato.

1. La richiesta di revoca da parte del terzo interessato da cui derivano i poteri di rappresentanza del titolare deve essere inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua decorrenza.

2. Il certificatore deve notificare la revoca al titolare.

3. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 21. Sospensione dei certificati qualificati.

1. La sospensione del certificato qualificato è effettuata dal certificatore attraverso l'inserimento di tale certificato in una delle liste dei certificati revocati e sospesi (CRL/CSL).

2. La sospensione dei certificati è annotata nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

Art. 22. Sospensione su iniziativa del certificatore.

1. Salvo casi d'urgenza, che il certificatore è tenuto a motivare contestualmente alla comunicazione di cui al comma 2, il certificatore che intende sospendere un certificato qualificato deve darne preventiva comunicazione al titolare specificando i motivi della sospensione e la sua durata.

2. L'avvenuta sospensione del certificato qualificato deve essere tempestivamente comunicata al titolare specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.

3. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione della sospensione.

Art. 23. Sospensione su richiesta del titolare.

1. La richiesta di sospensione deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua durata.

2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo.

3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal comma 2.

Art. 24. Sospensione su richiesta del terzo interessato.

1. La richiesta di sospensione da parte del terzo interessato, da cui derivano i poteri di rappresentanza del titolare, deve essere inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua durata.

2. Il certificatore deve notificare la sospensione al titolare.

Art. 25. Sostituzione delle chiavi di certificazione.

1. Almeno novanta giorni prima della scadenza del certificato relativo a chiavi di certificazione il certificatore deve avviare la procedura di sostituzione, generando, con le modalità previste dall'art. 13, una nuova coppia di chiavi.

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 risulti 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.

Art. 29. Accesso del pubblico ai certificati.

1. Le liste dei certificati revocati e sospesi devono essere rese pubbliche.

2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico, ovvero comunicati a terzi, esclusivamente nei casi consentiti dal titolare del certificato e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.

3. Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi le consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità della firma digitale.

Art. 30. Piano per la sicurezza.

1. Il certificatore deve definire un piano per la sicurezza nel quale devono essere contenuti almeno i seguenti elementi:

    a. struttura generale, modalità operativa e struttura logistica;

    b. descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza;

    c. allocazione dei servizi e degli uffici negli immobili;

    d. elenco del personale e sua allocazione negli uffici;

    e. attribuzione delle responsabilità;

    f. algoritmi crittografici o altri sistemi utilizzati;

    g. descrizione delle procedure utilizzate nell'attività di certificazione;

    h. descrizione dei dispositivi installati;

    i. descrizione dei flussi di dati;

    m. procedura di gestione delle copie di sicurezza dei dati;

    n. procedura di gestione dei disastri;

    o. analisi dei rischi;

    p. descrizione delle contromisure;

    q. specificazione dei controlli.

2. Fatto salvo quanto disposto al comma 3, il piano per la sicurezza, sottoscritto dal legale rappresentante del certificatore, deve essere consegnato al dipartimento in busta sigillata.

3. Le informazioni di cui al comma 1, lettere b), c) e d) devono essere consegnate al dipartimento in una busta sigillata, che verrà aperta solo in caso di contestazioni, diversa da quella nella quale è contenuto il piano per la sicurezza.

4. Il piano per la sicurezza deve attenersi quanto meno alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'art. 33, del decreto legislativo 30 giugno 2003, n. 196.

Art. 31. 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 associato un riferimento temporale.

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 devono essere conservate per un periodo non inferiore a 10 anni.

Art. 32. Sistema di qualità del certificatore.

1. Entro un anno dall'avvio dell'attività di certificazione, il certificatore deve dichiarare la conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti.

2. Il manuale della qualità deve essere depositato presso il dipartimento e reso disponibile presso il certificatore.

Art. 33. Organizzazione del personale del certificatore.

1. L'organizzazione del personale addetto al servizio di certificazione 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 o di altro sistema utilizzato;

   i. responsabile dei servizi tecnici;

   l. responsabile delle verifiche e delle ispezioni (auditing);

   m. responsabile del sistema di riferimento temporale.

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'art. 33 deve aver maturato una esperienza almeno quinquennale nell'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.

Art. 38. Manuale operativo.

1. Il manuale operativo definisce le procedure applicate dal certificatore che rilascia certificati qualificati nello svolgimento della sua attività.

2. Il manuale operativo deve essere depositato presso il dipartimento 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 dei richiedenti la verifica delle firme;

e. definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;

f. indirizzo del sito web del certificatore ove sono pubblicate le tariffe;

g. modalità di identificazione e registrazione degli utenti;

h. modalità di generazione delle chiavi per la creazione e la verifica della firma;

i. modalità di emissione dei certificati;

l. modalità con cui viene espletato quanto previsto all'art. 27-bis, comma 1, lettera a) del testo unico;

m. modalità di sospensione e revoca dei certificati;

n. modalità di sostituzione delle chiavi;

o. modalità di gestione del registro dei certificati;

p. modalità di accesso al registro dei certificati;

q. modalità di protezione della riservatezza;

r. modalità per l'apposizione e la definizione del riferimento temporale;

s. modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 10, comma 1;

t. modalità operative per la generazione della firma digitale.

Art. 39. Riferimenti temporali opponibili ai terzi.

1. I riferimenti temporali realizzati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 14, comma 2, del testo unico.

2. I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 14, comma 2, del testo unico.

3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al D.M. 30 novembre 1993, n. 591 del Ministro dell'industria, del commercio e dell'artigianato, con una differenza non superiore ad un minuto primo.

4. Le pubbliche amministrazioni possono anche utilizzare come sistemi di validazione temporale:

   a. il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella 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'art. 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'art. 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'art. 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'art. 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'art. 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'art. 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'art. 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.

TITOLO IV

Regole per la validazione temporale e per la protezione dei documenti informatici.

Art. 44. 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:

mantenere la data e l'ora conformemente a quanto richiesto dal presente decreto;

generare la struttura di dati secondo quanto specificato negli articoli 45 e 48;

sottoscrivere digitalmente la struttura di dati di cui alla lettera b).

Art. 45. 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 al comma 1, lettera g).

Art. 46. 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 ed un nuovo certificato deve essere emesso 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 appositamente generate.

4. Le chiavi di certificazione e di marcatura temporale possono essere generate esclusivamente dai responsabili dei rispettivi servizi.

Art. 47. Gestione dei certificati e delle chiavi.

1. Alle chiavi di certificazione utilizzate, ai sensi dell'art. 46, comma 3, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.

2. I certificati relativi ad una coppia di chiavi di marcatura temporale, oltre ad essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni, devono contenere l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 48. 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 D.M. 30 novembre 1993, n. 591 del Ministro dell'industria, del commercio e dell'artigianato, al momento della sua generazione.

2. La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato (UTC).

Art. 49. 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 all'art. 48, comma 1, 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 criteri di sicurezza almeno equivalenti a quelli previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC, o dal livello EAL 3 della norma ISO/IEC 15408 o superiori. Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

Art. 50. Registrazione delle marche generate.

1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a cinque anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.

2. La marca temporale è valida per l'intero periodo di conservazione a cura del fornitore del servizio.

Art. 51. 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 basate sugli 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.

4. Il certificatore ha facoltà di implementare il sistema di validazione temporale in modo che sia possibile richiedere 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. 52. 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 marca temporale.

TITOLO V

Disposizioni finali e transitorie.

Art. 53. Norme transitorie.

1. In attesa della pubblicazione degli algoritmi per la generazione e verifica della firma digitale secondo quanto previsto dall'art. 3, i certificatori accreditati ai sensi dell'art. 28 del testo unico, devono utilizzare l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 1024 bit.

2. In attesa della pubblicazione delle funzioni di hash secondo quanto previsto dall'art. 3, i certificatori accreditati ai sensi dell'art. 28 del testo unico devono utilizzare uno dei seguenti algoritmi, definiti nella norma ISO/IEC 10118-3:1998 e successive evoluzioni:

    a. dedicated hash-function 3, corrispondente alla funzione SHA-1;

    b. dedicated hash-function 1, corrispondente alla funzione RIPEMD-160.

3. In attesa che la Commissione europea, secondo la procedura di cui all'art. 9 della direttiva 1999/93/CE, indichi i livelli di valutazione relativamente alla certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma prevista dall'art. 10 del decreto legislativo 23 gennaio 2002, n. 10, tale certificazione è effettuata secondo criteri non inferiori a quelli previsti dal livello di 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 dal Centro nazionale per l'informatica nella pubblica amministrazione.

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 nella Gazzetta Ufficiale 15 aprile 1999, n. 87.

14.3 DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 12 ottobre 2007 – Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'articolo 13, comma 4, del decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003 (G.U. 16-1-2008, n.13).

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera *mm)*, della legge 23 ottobre 1992, n. 421;

Vista la direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche e, in particolare, l'allegato III, così come modificato in esito alla rettifica pubblicata nella Gazzetta Ufficiale delle Comunità europee serie L 13 del 19 gennaio 2000;

Vista la decisione della Commissione europea 2003/511/CE del 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;

Visto il proprio decreto del 30 ottobre 2003, pubblicato sulla Gazzetta Ufficiale del 27 aprile 2004, n. 98, recante approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore delle tecnologie dell'informazione, ai sensi dell'articolo 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10;

Visto il proprio decreto del 13 gennaio 2004, pubblicato sulla Gazzetta Ufficiale del 27 aprile 2004, n. 98, recante regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione anche temporale dei documenti informatici;

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante Codice dell'amministrazione digitale, e, in particolare, gli articoli 31, 35 e 71;

Visto il proprio decreto del 15 giugno 2006, recante delega di funzioni del Presidente del Consiglio dei Ministri in materia di riforme e innovazioni nella pubblica amministrazione al Ministro senza portafoglio, prof. Luigi Nicolais;

Considerata la complessità nella definizione dei tempi e dei costi di mercato delle procedure di certificazione di cui al citato decreto del 30 ottobre 2003 e la conseguente indisponibilità, allo stato attuale, di dispositivi sicuri per la creazione della firma certificati secondo le norme vigenti, da utilizzare nelle procedure automatiche di cui all'articolo 35, comma 3, del decreto legislativo n. 82 del 2005;

Ritenuta la necessità di consentire l'utilizzo di dispositivi sicuri per l'apposizione di firme con procedure automatiche, anche per la fatturazione elettronica;

Considerata, quindi l'esigenza di differire ulteriormente il termine entro il quale i certificatori qualificati attestano, mediante autodichiarazione, la rispondenza dei propri prodotti e dispositivi relativi alle firme elettroniche da apporre con procedure automatiche ai requisiti di sicurezza definiti dalla vigente normativa, fermo restando lo svolgimento dell'attività di vigilanza prevista dalla stessa;

Sentito il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA);

Di concerto con i Ministri delle comunicazioni, dello sviluppo economico e dell'economia e delle finanze;

DECRETA

Art. 1

1. Per un periodo di ventiquattro mesi decorrente dall'entrata in vigore del presente decreto, i certificatori di firma elettronica attestano, mediante autodichiarazione, la rispondenza dei propri prodotti e dispositivi relativi alle firme elettroniche da apporre con procedure automatiche ai requisiti di sicurezza previsti dalla vigente normativa.
2. Le autodichiarazioni già rese ai sensi del D.P.C.M. 7 dicembre 2000, del D.P.C.M. 20 aprile 2001, del D.P.C.M. 3 ottobre 2001 e del D.P.C.M. 30 ottobre 2003, relative ai dispositivi sicuri per l'apposizione di firme con procedure automatiche, continuano a spiegare ininterrottamente i propri effetti fino al termine del periodo di cui al comma 1.
3. Le attestazioni di cui al comma 1 rientrano nell'ambito di applicazione delle funzioni di vigilanza e controllo svolte dal CNIPA sull'attività dei certificatori qualificati e accreditati, ai sensi dell'articolo 31 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.
4. Il presente decreto non reca oneri aggiuntivi per il bilancio dello Stato.

Il presente decreto è inviato ai competenti organi di controllo e sarà pubblicato sulla Gazzetta Ufficiale della Repubblica italiana.

Capitolo 15 Norme attuative del CNIPA

15.1 Deliberazione 17 febbraio 2005, n. 4 – Regole per il riconoscimento e la verifica del documento informatico

Titolo I
DISPOSIZIONI GENERALI
IL COLLEGIO

Visto il decreto legislativo 12 febbraio 1993, n. 39, così come modificato dall'art. 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;

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;

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'art. 40, comma 4, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004;

Delibera

di emanare le seguenti regole per il riconoscimento e la verifica del documento informatico.

Art. 1. Definizioni

1. Fatte salve le definizioni contenute negli articoli 1 e 22 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni, ai fini delle presenti regole si intende 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) regole tecniche, le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici emanate con decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 pubblicate nella Gazzetta Ufficiale 27 aprile 2004, n. 98;

   c) firme multiple, firme digitali apposte da diversi sottoscrittori allo stesso documento;

   d) campo, unità informativa contenuta nel certificato. Può essere composta da diverse unità informative elementari dette «attributi»;

   e) estensione, metodo utilizzato per associare specifiche informazioni (attributi) alla chiave pubblica contenuta nel certificato, utilizzata per fornire ulteriori informazioni sul titolare del certificato e per gestire la gerarchia di certificazione;

   f) attributo, informazione elementare contenuta in un campo di un certificato elettronico come un nome, un numero o una data;

   g) attributi autenticati, insieme di attributi sottoscritti con firma elettronica dal sottoscrittore;

h) marcatura critica, caratteristica che possono assumere le estensioni conformemente allo standard RFC 3280;

i) marca temporale, un'evidenza informatica che consente la validazione temporale;

l) OID (Object Identifier), codice numerico standard per l'identificazione univoca di evidenze informatiche utilizzate per la rappresentazione delle strutture di dati nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti;

m) RFC (Request For Comments), documenti contenenti specifiche tecniche standard, riconosciute a livello internazionale, definite dall'Internet Engineering Task Force (IETF) e dall'Internet Engineering Steering Group (IESG);

n) ETSI (European Telecommunications Standards Institute), organizzazione indipendente, no profit, la cui missione è produrre standard sulle telecomunicazioni. È ufficialmente responsabile per la creazione di standard in Europa;

o) HTTP (Hypertext Transfer Protocol), protocollo per il trasferimento di pagine ipertestuali e risorse in rete conforme allo standard RFC 2616 e successive modificazioni;

p) LDAP (Lightweight Directory Access Protocol), protocollo di rete utilizzato per rendere accessibili informazioni in rete conforme allo standard RFC 3494 e successive modificazioni.

Art. 2. Ambito di applicazione e contenuto

1. La presente deliberazione stabilisce, ai sensi dell'art. 40, comma 4 delle regole tecniche, le regole per il riconoscimento e la verifica del documento informatico cui i certificatori accreditati devono attenersi al fine di ottenere e mantenere il riconoscimento di cui all'art. 28, comma 1 del testo unico.

2. Le disposizioni di cui al titolo II definiscono il formato dei certificati qualificati e le informazioni che in essi devono essere contenute.

3. Le disposizioni di cui al titolo III definiscono il formato dei certificati elettronici di certificazione e le informazioni che in essi devono essere contenute, generati ai sensi dell'art. 13, comma 2, delle regole tecniche, e il formato dei certificati elettronici di marcatura temporale e le informazioni che in essi devono essere contenute.

4. Le disposizioni di cui al titolo IV definiscono il formato e le informazioni che devono essere contenute nelle marche temporali utilizzate dai sistemi di validazione temporale dei documenti, così come definiti nel titolo IV delle regole tecniche.

5. Le disposizioni di cui al titolo V definiscono i formati e le modalità di accesso alle informazioni sulla revoca e la sospensione dei certificati, ai sensi dell'art. 29, comma 1, delle regole tecniche.

6. Le disposizioni di cui al titolo VI definiscono i formati delle buste crittografiche destinate a contenere gli oggetti sottoscritti con firma digitale.

7. Le disposizioni di cui al titolo VII definiscono i requisiti delle applicazioni di verifica della firma digitale di cui all'art. 10 delle regole tecniche.

Titolo II – PROFILO DEI CERTIFICATI QUALIFICATI

Art. 3. Norme generali

1. Il profilo dei certificati è, se non diversamente indicato, conforme alla specifica RFC 3280, capitolo 4, recante «Profilo dei certificati e delle liste di revoca dei certificati nell'infrastruttura a chiave pubblica» e, se non diversamente indicato, conforme alla specifica ETSI TS 101 862 V1.3.2, recante «Profilo dei certificati qualificati».

Art. 4. Profilo dei certificati qualificati

1. Salvo quanto diversamente disposto nella presente deliberazione, ai certificati qualificati si applica quanto stabilito nella specifica ETSI TS 102 280 V1.1.1, recante «Profilo dei certificati X.509 V.3 per certificati rilasciati a persone fisiche».

2. Il campo Issuer (emittente) del certificato contiene almeno i seguenti attributi:

   a) organizationName (OID: 2.5.4.10), che contiene la ragione sociale o denominazione dell'organizzazione che emette il certificato qualificato;

   b) countryName (OID: 2.5.4.6), che contiene il country code ISO 3166 dello Stato in cui è registrata l'organizzazione indicata nell'organizationName.

3. Il campo SubjectDN (Dati identificativi del titolare) del certificato contiene i seguenti attributi:

   a) givenName e surname (OID: 2.5.4.42 e 2.5.4.4) che contengono rispettivamente nome di battesimo e cognome del titolare del certificato;

   b) countryName (OID: 2.5.4.6) che, nel caso in cui l'organizationName contenga il valore «non presente», contiene il country code ISO 3166 dello Stato di residenza del titolare. Nel caso in cui l'organizationName contenga un valore diverso da «non presente», contiene il country code ISO 3166 dello Stato che ha assegnato all'organizzazione il codice identificativo riportato nell'attributo organizationName;

   c) organizationName (OID: 2.5.4.10) che contiene, se applicabile, la ragione sociale o la denominazione e il codice identificativo dell'organizzazione che ha richiesto o autorizzato il rilascio del certificato del titolare. Il codice identificativo è un codice rilasciato dall'autorità governativa preposta dello Stato indicato nell'attributo countryName. Se l'organizationName non è applicabile, assume il valore «non presente»;

   d) serialNumber (OID: 2.5.4.5) che contiene il codice fiscale del titolare rilasciato dall'autorità fiscale dello Stato di residenza del titolare o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. Allo scopo di definire il contesto per la comprensione del codice in questione, il codice stesso è preceduto dal country code ISO 3166 e dal carattere «:» (in notazione esadecimale «0x3A»);

   e) in alternativa agli attributi specificati alla lettera a), il certificato può contenere l'attributo pseudonym (OID: 2.5.4.65), che contiene una qualsiasi stringa univoca, a discrezione del titolare. La stringa utilizzata non permette di risalire ai dati identificativi del titolare. Se l'attributo pseudonym è presente, l'attributo countryName assume il valore «IT», l'attributo organizationName assume il valore «non presente», l'attributo serialNumber il valore «pseudonimo» e gli attributi title e localityName non sono presenti;

f) dnQualifier (OID: 2.5.4.46), contiene il codice identificativo del titolare presso il certificatore. Detto codice, assegnato dal certificatore, è univoco.

4. Il campo subjectDN (Dati identificativi del titolare) del certificato può contenere altri attributi purché non in contrasto con quanto previsto dal documento ETSI TS 102 280. L'eventuale codifica degli attributi title, localityName, commonName e organizational UnitName rispetta le seguenti regole:

   a) title (OID: 2.5.4.12), contiene una indicazione della qualifica specifica del titolare, quale l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, ovvero i poteri di rappresentanza nell'ambito dell'organizzazione specificata nell'attributo organizationName. Nel caso in cui l'attributo organizationName contenga un valore diverso da «non presente», l'inserimento delle informazioni nel title è richiesto dall'organizzazione stessa. In caso contrario contiene informazioni derivanti da autocertificazione effettuata dal titolare ai sensi della normativa vigente;

   b) localityName (OID: 2.5.4.7), contiene, nel caso in cui l'attributo organizationName contenga un valore diverso da «non presente», informazioni pertinenti all'organizzazione specificata;

   c) commonName (OID: 2.5.4.3), in aggiunta a surname e givenName, contiene l'eventuale altro nome con il quale il titolare è comunemente conosciuto;

   d) organizationalUnitName (OID: 2.5.4.11), contiene ulteriori informazioni inerenti all'organizzazione. Tale attributo può comparire, al massimo, cinque volte.

5. Il certificato contiene inoltre le seguenti estensioni:

   a) keyUsage (OID: 2.5.29.15) che contiene esclusivamente il valore nonRepudiation (bit 1 impostato a 1). L'estensione è marcata critica;

   b) certificatePolicies (OID: 2.5.29.32) che contiene l'OID della Certificate Policy (CP) e l'Uniform Resource Locator (URL) che punta al Certificate Practice Statement (CPS) nel rispetto del quale il certificatore ha emesso il certificato. Se non viene adottata una CP
   definita a livello nazionale o europeo, il certificatore definisce una propria CP e tale OID è definito e pubblicizzato dal certificatore. Possono essere indicate più Certificate Policy (CP). L'URL configura un percorso assoluto per l'accesso alla CRL. L'estensione non è marcata critica;

   c) CRLDistributionPoints (OID: 2.5.29.31) che contiene l'URL che punta alle CRL/CSL pubblicate dal certificatore dove eventualmente saranno disponibili le informazioni relative alla revoca o sospensione del certificato in questione. L'URL configura un percorso assoluto per l'accesso alla CRL. Lo schema da utilizzare per l'URL è
   HTTP oppure LDAP e consente lo scaricamento anonimo della CRL. Nel caso vengano valorizzati più di un URL per l'estensione, tali URL configurano percorsi coerenti con l'ultima CRL/CSL pubblicata. L'estensione non è marcata critica;

   d) authorityKeyIdentifier (OID: 2.5.29.35) che contiene almeno l'attributo keyIdentifier. L'estensione non è marcata critica;

   e) subjectKeyIdentifier (OID: 2.5.29.14) che contiene almeno l'attributo keyIdentifier. L'estensione non è marcata critica;

   f) qcStatements, identificate nel documento ETSI TS 101 862 come segue:

      1) id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1);

      2) id-etsi-qcs-QcLimitValue (OID: 0.4.0.1862.1.2), presente se sono applicabili limiti nelle negoziazioni;

      3) id-etsi-qcs-QcRetentionPeriod (OID: 0.4.0. 1862.1.3), il valore indicato è pari o superiore a «10»;

4) id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4).

L'estensione non è marcata critica.

6. Il certificato di sottoscrizione può contenere le seguenti estensioni:

a) SubjectDirectoryAttributes (OID: 2.5.29.9).

Essa non contiene alcuno dei campi indicati ai commi 3 e 4. L'attributo dateOfBirth (OID: 1.3.6.1.5.5.7.9.1), se presente, è codificato nel formato GeneralizedTime. L'estensione non è marcata critica;

b) authorityInfoAccess (OID: 1.3.6.1.5.5.7.1.1).
Nel caso in cui il certificatore metta a disposizione, conformemente all'art. 10, un sistema OCSP per la verifica della validità di un certificato, l'estensione Authority InfoAccess contiene un campo accessDescription con la descrizione delle modalità di accesso al servizio OCSP, e contiene i seguenti attributi:

1) accessMethod, che contiene l'identificativo id-ad-ocsp (OID: 1.3.6.1.5.5.7.48.1);

2) accessLocation, che contiene l'URI che punta all'OCSP Responder del certificatore, utilizzabile per effettuare la verifica del certificato stesso. L'URI configura un percorso assoluto per l'accesso all'OCSP Responder.
Nel caso in cui siano specificati più campi access Description contenenti l'identificativo id-ad-ocsp nell'attributo accessMethod, tali indicazioni configurano diversi percorsi alternativi per l'interrogazione, tramite OCSP, dello stato del certificato.

L'estensione non è marcata critica;

c) salvo quanto disposto all'art. 4, comma 5, lettera f), gli eventuali ulteriori limiti d'uso di cui all'art. 43 delle regole tecniche sono inseriti nell'attributo explicitText del campo userNotice dell'estensione certificatePolicies;

d) ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nella presente deliberazione e non marcate critiche.

Titolo III

PROFILO DEI CERTIFICATI DI CERTIFICAZIONE E MARCATURA TEMPORALE

Art. 5. Profilo dei certificati di certificazione e marcatura temporale

1. Se non diversamente previsto, il profilo dei certificati è conforme alla specifica RFC 3280.

Art. 6. Uso delle estensioni nei certificati di certificazione

1. I certificati di certificazione contengono le seguenti estensioni:

a) keyUsage (OID 2.5.29.15), contiene i valori keyCertSign e cRLSign (bit 5 e 6 impostati a 1). L'estensione è marcata critica;

b) basicConstraints (OID 2.5.29.19), contiene il valore CA=true. L'estensione è marcata critica;

c) certificatePolicies (OID 2.5.29.32), contiene uno o più identificativi delle policyIdentifier e le relative URL del CPS. Può contenere l'OID generico previsto dall'RFC 3280 (2.5.29.32.0). L'estensione non è marcata critica;

d) CRLDistributionPoints (OID 2.5.29.31), contiene uno o più URL di accesso a CRL/CSL. L'URL configura un percorso assoluto per l'accesso alla CRL. L'estensione non è marcata critica;

e) subjectKeyIdentifier (OID 2.5.29.14), contiene il valore keyIdentifier. L'estensione non è marcata critica.

2. Ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nella presente deliberazione e non marcate «critiche».

Art. 7. Uso delle estensioni nei certificati di marcatura temporale

1. I certificati di marcatura temporale contengono le seguenti estensioni:

a) keyUsage (OID 2.5.29.15), contiene il valore digitalSignature (bit 0 impostato a 1). L'estensione è marcata critica;

b) extendedKeyUsage (OID 2.5.29.37), contiene il valore keyPurposeId=timeStamping. L'estensione è marcata critica;

c) certificatePolicies OID 2.5.29.32), contiene uno o più identificativi delle policyIdentifier e le relative URL del CPS. L'estensione non è marcata critica;

d) authorityKeyIdentifier (OID 2.5.29.35), contiene almeno un keyIdentifier. L'estensione non è marcata critica;

e) subjectKeyIdentifier (OID 2.5.29.14), contiene almeno un keyIdentifier. L'estensione non è marcata critica.

2. Ulteriori estensioni possono essere inserite nel certificato purché conformemente agli standard citati nella presente deliberazione e non marcate «critiche».

Titolo IV

REGOLE PER LA VALIDAZIONE TEMPORALE

Art. 8. Regole per i servizi di validazione temporale

1. L'accesso al servizio di validazione temporale fornito dai certificatori avviene tramite il protocollo e il formato definiti nella specifica ETSI TS 101 861 V.1.2.1, recante «Profilo di validazione temporale» e nella specifica RFC 3161 e successive modificazioni. Le marche temporali inviate in risposta al richiedente seguono i medesimi standard.

2. I certificatori rendono disponibile o indicano un sistema che permetta l'apertura, l'analisi e la visualizzazione di marche temporali di cui al comma 1. Detto sistema gestisce correttamente le strutture TimeStampToken e TimeStampResp almeno nel formato detached, con verifica della firma del sistema di validazione temporale e della corretta associazione, effettuata tramite la funzione di hash, con il documento per il quale è stata generata la marca temporale stessa.

3. L'estensione associata alla struttura TimeStampToken e TimeStampResp non deve influire sul corretto funzionamento del sistema di cui al comma 2.

4. I TimeStampToken devono includere un identificativo univoco della policy di sicurezza in base alla quale il token stesso è stato generato. Detto identificativo, se non definito a livello nazionale od europeo, è definito e reso pubblico dal certificatore.

Titolo V

INFORMAZIONI SULLA REVOCA E SOSPENSIONE DEI CERTIFICATI

Art. 9. Verifica dei certificati – CRL

1. Le informazioni sulla revoca e sospensione dei certificati, pubblicate dai certificatori e disponibili pubblicamente tramite liste di revoca e sospensione, hanno un formato conforme alla specifica RFC 3280, capitolo 5, esclusi i paragrafi 5.2.4 e 5.2.6.

2. Le liste di certificati revocati e sospesi sono accessibili al pubblico tramite protocollo HTTP o LDAP.

Art. 10. Verifica in tempo reale dei certificati – OCSP

1. Fermo restando quanto prescritto dall'art. 9, i certificatori hanno la facoltà di rendere disponibili le informazioni sulla revoca e sospensione dei certificati, anche attraverso servizi OCSP. In tal caso, detti servizi devono essere conformi alle specifica RFC 2560 e successive modificazioni.

Art. 11. Coerenza delle informazioni sulla revoca e sospensione dei certificati

1. Se un certificatore mette a disposizione diversi servizi per l'accesso alle informazioni sulla revoca o la sospensione dei certificati, o diversi URL di accesso allo stesso servizio, le informazioni ottenute accedendo con le diverse modalità devono essere coerenti se ciò è compatibile con la tecnologia utilizzata.

Titolo VI

FORMATI DI FIRMA

Art. 12. Busta crittografica di firma

1. La busta crittografica destinata a contenere l'oggetto sottoscritto è conforme, salvo i casi previsti dai commi 8 e 9, alla specifica RFC 2315 (PKCS7 ver. 1.5).

2. La busta crittografica di cui al comma 1 è di tipo signedData (OID: 1.2.840.113549.1.7.2).

3. Per la codifica della busta crittografica possono essere utilizzati i formati ASN.1-DER (ISO 8824, 8825) o BASE64 (RFC 1421).

4. Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso.

5. Il nome del file firmato, ossia della busta, assume l'ulteriore estensione «p7m».

6. Le buste crittografiche di cui al comma 5 possono contenere a loro volta buste crittografiche. In questo caso è applicata una ulteriore estensione «p7m».

7. L'eventuale presenza di attributi autenticati nella busta crittografica non è considerata critica. La gestione degli stessi non deve rappresentare un vincolo per le applicazioni di verifica di cui all'art. 14.

8. Il CNIPA può stabilire, con apposito provvedimento, ulteriori formati standard di busta crittografica, riconosciuti a livello nazionale o internazionale, conformi a specifiche pubbliche (Publicly Available Specification-PAS).

9. Il CNIPA può sottoscrivere specifici protocolli d'intesa al fine di rendere disponibili ulteriori formati di firma. Detti protocolli d'intesa devono contenere l'impegno del sottoscrittore ad assicurare:

    a) la disponibilità delle specifiche necessarie per lo sviluppo di prodotti di verifica o di generazione e eventuali librerie software necessarie per lo sviluppo di prodotti di verifica di firme digitali conformi al formato oggetto del protocollo d'intesa;

    b) l'assenza di qualunque onere finanziario a carico di chi sviluppa, distribuisce o utilizza i prodotti menzionati al comma precedente;

    c) la disponibilità di ogni modifica inerente a quanto indicato alla lettera a) con un anticipo di almeno 90 giorni rispetto alla data del rilascio di nuove versioni del prodotto che implementa il formato di busta crittografica oggetto del protocollo d'intesa;

    d) la disponibilità, a titolo gratuito per uso personale, di un prodotto per verificare firme digitali del formato oggetto del protocollo d'intesa e visualizzare il documento informatico oggetto della sottoscrizione;

    e) la capacità di utilizzare le informazioni contenute nell'elenco pubblico dei certificatori di cui all'art. 41 delle regole tecniche e nelle liste di revoca di cui all'art. 29 del citato provvedimento nel prodotto di verifica di cui al comma precedente.

10. Fermo restando il rispetto delle condizioni previste al comma 9, il CNIPA, consultando preventivamente le autorità di settore e le associazioni di categoria maggiormente rappresentative, valuta le richieste di sottoscrizione dei protocolli d'intesa previsti dal comma sopra citato avendo riguardo:

    a) alla rilevanza delle esigenze che essi consentono di soddisfare;

    b) alla possibilità di assicurare un idoneo supporto e un'adeguata diffusione sul mercato nazionale ed internazionale dei prodotti che realizzano la struttura informatica del documento sottoscritto, tali da essere riconosciuti ed accettati quali standard di riferimento;

    c) alla necessità di evitare effetti negativi sulla interoperabilità.

11. Le pubbliche amministrazioni possono accettare documenti informatici sottoscritti con i formati di firma di cui ai commi 8 e 9 e, nel caso ritengano opportuno accettare uno o più di detti formati, dovranno farne apposita menzione nei procedimenti amministrativi cui si applicano e comunicarlo al CNIPA. Le pubbliche amministrazioni garantiscono la gestione del formato di cui al comma 1.

12. Il soggetto che sottoscrive il protocollo d'intesa di cui al comma 9 indica al CNIPA gli indirizzi internet dove è possibile ottenere, gratuitamente e liberamente, quanto indicato alle lettere a) e d) del medesimo comma 9.

13. Il CNIPA rende disponibili sul proprio sito internet: l'elenco dei formati oggetto di protocolli d'intesa, gli indirizzi internet di cui al comma 12 e gli eventuali formati di busta crittografica di cui al comma 8.

14. In caso di inadempienza da parte del sottoscrittore del protocollo d'intesa di quanto previsto ai commi 9 e 12, il CNIPA informa tempestivamente il soggetto interessato e, nel caso lo stesso non ottemperi rapidamente alla piena osservanza di quanto previsto, revoca il protocollo d'intesa dandone

pubblicità nell'elenco di cui al comma 13 ed informandone tempestivamente le pubbliche amministrazioni di cui al comma 11.

Art. 13. Regole per l'apposizione di firme multiple

1. Una stessa busta crittografica può contenere più firme digitali. Queste ultime sono identificate in:

    a) «Firme parallele», in tal caso il sottoscrittore, utilizzando la propria chiave privata, firma solo i dati contenuti nella busta stessa (OID: 1.2.840.113549.1.7.1) ;

    b) «Controfirme», in tal caso il sottoscrittore, utilizzando la propria chiave privata, firma una precedente firma (OID: 1.2.840.113549.1.9.6) apposta da altro sottoscrittore.

2. Il formato delle firme multiple definite nel presente articolo è conforme alla specifica RFC 2315.

3. L'apposizione di firme multiple di cui al presente articolo non comporta l'applicazione di ulteriori estensioni al file firmato, oltre alla prima.

Titolo VII

APPLICAZIONI DI VERIFICA DELLA FIRMA

Art. 14. Requisiti delle applicazioni di verifica

1. Le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati, ai sensi dell'art. 10 delle regole tecniche, oltre a gestire correttamente i certificati elettronici il cui formato è stabilito nella presente deliberazione, riconoscono i seguenti elementi dei certificati qualificati:

    a) l'attributo DateOfBirth dell'estensione SubjectDirectoryAttributes;

    b) le seguenti qcStatements:

        1) id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1);

        2) id-etsi-qcs-QcLimitValue (OID: 0.4.0.1862.1.2);

        3) id-etsi-qcs-QcRetentionPeriod (OID: 0.4.0.1862. 1.3);

        4) id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4).

2. Oltre a quanto prescritto al precedente comma 1, le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati gestiscono i formati di firma e le buste crittografiche di cui all'art. 12, commi da 1 a 7, e all'art. 13.

3. Le applicazioni di cui al presente articolo gestiscono correttamente il processo di verifica delle firme digitali prodotte precedentemente all'entrata in vigore della presente deliberazione
che non perdono la loro specifica validità.

Titolo VIII

DISPOSIZIONI FINALI E TRANSITORIE

Art. 15. Operatività

1. La presente deliberazione entra in vigore a decorrere da nove mesi dalla data di pubblicazione nella Gazzetta Ufficiale.

2. L'obbligo di utilizzo della codifica UTF-8, previsto nella RFC 3280, ha effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione.

3. L'obbligo di cui all'art. 4, comma 5, lettera f) ha effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione. Fino a tale data, se il certificato non contiene nell'estensione qcStatement i valori id-etsi-qcs-QcCompliance e id-etsi-qcs-QcSSCD, almeno una delle policy indicate nel certificato indica esplicitamente che il certificato è un certificato qualificato e che la chiave privata, corrispondente alla chiave pubblica presente nel certificato qualificato, è memorizzata su un dispositivo sicuro per la generazione della firma conforme alle
normative vigenti.

4. Durante il periodo di proroga di cui al comma 3, se il certificato non contiene nell'estensione qcStatement il valore id-etsi-qcs-QcLimitValue, gli eventuali limiti di negoziazione sono
inseriti nell'attributo explicitText del campo userNotice.

5. Le disposizioni di cui all'art. 14 hanno effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione.

6. I certificati elettronici emessi precedentemente all'entrata in vigore della presente deliberazione rimangono validi fino alla scadenza prevista al momento dell'emissione, salvo precedente revoca o sospensione.

15.2 Circolare 6 settembre 2005, n. 48

Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Con la presente circolare vengono indicate le modalità con le quali i soggetti - pubblici e privati - che intendono presentare domanda di accreditamento ai sensi dell'art. 28 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (di seguito indicato «Testo unico») - come sostituito dall'art. 13 del decreto del Presidente della Repubblica 7 aprile 2003, n. 137, devono presentare domanda al Centro nazionale per l'informatica nella pubblica amministrazione (di seguito indicato «CNIPA»).

La domanda di accreditamento, sottoscritta dal legale rappresentante della pubblica amministrazione o della società richiedente, corredato degli allegati di seguito indicati, deve essere inviata - in plico chiuso con l'indicazione del mittente – al CNIPA, via Isonzo 21b - 00198 Roma. La consegna può avvenire tramite servizio pubblico o privato oppure a mano nelle ore d'ufficio (9-13 e 15-17) dei giorni feriali, dal lunedì al venerdì. In caso di consegna a mano, verrà rilasciata ricevuta dell'avvenuta consegna del plico.

La domanda deve indicare:

a) la denominazione o la ragione sociale;

b) la sede legale;

c) le sedi operative;

d) il/i rappresentante/i legale/i;

e) l'elenco dei documenti allegati.

È opportuno che in detta domanda siano indicati anche il nominativo e i recapiti (numeri telefonici, numeri di telefax, indirizzo di posta elettronica) di un referente cui rivolgersi in presenza di problematiche di minore importanza che possono essere risolte per le vie brevi.

Al fine di dimostrare il possesso dei requisiti previsti dagli articoli 27 e 28, comma 3, del testo unico e di ottemperare a quanto previsto dall'art. 11, comma 1, e dagli articoli 30, 34 e 38 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, recante: «Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici» - fatta salva la facoltà di avvalersi delle dichiarazioni sostitutive previste dal citato testo unico - alla domanda deve essere allegata la seguente documentazione:

a) copia autentica dell'atto costitutivo della società;

b) copia dello statuto sociale aggiornato, rilasciato dalla competente CCIAA in data non anteriore a novanta giorni rispetto a quella di presentazione della domanda stessa;

c) certificato di iscrizione nel registro delle imprese con dicitura antimafia, rilasciato in data non anteriore a novanta giorni rispetto a quella di presentazione della domanda;

d) dichiarazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile ai sensi della normativa vigente - di data non anteriore a trenta giorni rispetto a quella di presentazione della domanda - attestante l'entità del capitale sociale versato, nonché l'ammontare e la composizione del patrimonio netto;

e) situazione patrimoniale, predisposta e approvata dall'organo amministrativo, di data non anteriore a centottanta giorni rispetto a quella di presentazione della domanda (solo per le società già operative);

f) relazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile, redatta ai sensi della normativa vigente, sulla situazione patrimoniale di cui alla lettera e);

g) documentazione equivalente a quella prevista ai punti precedenti, legalizzata ai sensi dell'art. 33 del testo unico (per le società costituite all'estero ed aventi sede in Italia);

h) elenco nominativo dei rappresentanti legali, dei componenti dell'organo di amministrazione e dell'organo di controllo, nonché di eventuali altri soggetti preposti all'amministrazione, con l'indicazione dei relativi poteri. Ognuno dei suddetti soggetti, dovrà risultare in possesso, all'atto della domanda, dei requisiti di onorabilità di cui all'art. 28, comma 3, lettera b), del testo unico, comprovato:

- per i cittadini italiani residenti in Italia: - dalla dichiarazione sostitutiva di atto di notorietà, circa il possesso dei requisiti di cui all'art. 28 del testo unico; - dal certificato del casellario giudiziale; - dal certificato relativo ai carichi pendenti;

- per le persone che non rientrano nella categoria di cui al precedente alinea: - dalla dichiarazione, resa davanti a pubblico ufficiale, di possedere i requisiti di cui all'art. 28 del testo unico; - dai certificati attestanti che il soggetto non è fallito o sottoposto a procedura equivalente;

Le firme apposte sulla documentazione anzidetta devono essere legalizzate con le modalità di cui al testo unico.

In alternativa, per i soggetti iscritti nell'albo di cui all'art. 13 del decreto legislativo 1° settembre 1993, n. 385, recante: «Testo unico delle leggi in materia bancaria e creditizia» - la dimostrazione del possesso dei requisiti di onorabilità da parte delle persone di cui alla presente lettera, potrà essere assolta mediante apposita dichiarazione sostitutiva di certificazione resa, ai sensi dell'art. 46 del Testo unico, dal legale rappresentante, attestante l'iscrizione nel suddetto albo alla data di presentazione della domanda di accreditamento;

i) copia della polizza assicurativa (o certificato provvisorio impegnativo) stipulata per la 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;

l) copia dell'ultimo bilancio e relativa certificazione, se la società è stata costituita da più di un anno;

m) dichiarazione, rilasciata dal presidente della società, attestante la composizione dell'azionariato, per quanto nota, con l'indicazione, comunque, dei soggetti partecipanti, in forma diretta o indiretta, al capitale sociale in misura superiore al 5%;

n) copia del manuale operativo sottoscritto da soggetto munito di potere di firma;

o) copia del piano per la sicurezza, sottoscritto e siglato in ogni foglio da soggetto munito di potere di firma;

p) una relazione sulla struttura organizzativa, debitamente sottoscritta dal legale rappresentante;

q) dichiarazione di disponibilità a consentire l'accesso di incaricati del CNIPA presso le strutture dedicate alle operazioni di certificazione, al fine di potere verificare la permanenza dei requisiti tecnico-organizzativi documentati all'atto della presentazione della domanda;

r) dichiarazione di impegno a comunicare al CNIPA le caratteristiche dei «dispositivi sicuri per la creazione della firma» che si intende fornire nello svolgimento del servizio;

s) dichiarazione d'impegno a comunicare al CNIPA ogni eventuale variazione intervenuta, con riguardo a quanto dichiarato all'atto della presentazione della domanda di accreditamento. A seguito di tali comunicazioni il CNIPA può procedere ad una nuova - se del caso anche parziale - valutazione dei requisiti o richiedere ulteriore documentazione;

t) dichiarazione d'impegno a rispettare quanto prescritto dall'art. 53, comma 4, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 e successive modificazioni.

Le pubbliche amministrazioni dovranno allegare solo la documentazione di cui alle lettere n), o), p), q), r), s) e t).

Ai sensi dell'art. 29-bis, comma 2, lettera f), del testo unico e dell'art. 11, comma 1, lettera i), del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, alla domanda va altresì allegata apposita dichiarazione tecnica contenente quanto segue:

a) algoritmi di generazione e di verifica delle firme utilizzati e supportati dal certificatore;

b) algoritmi di hash utilizzati e supportati dal certificatore;

c) lunghezza delle chiavi;

d) garanzie 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 alle informazioni di revoca e di sospensione 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;

l) caratteristiche del sistema di generazione dei certificati;

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

n) modalità di tenuta del giornale di controllo;

o) descrizione del sistema di validazione temporale adottato;

p) impegno ad adottare ogni opportuna misura tecnico-organizzativa volta a garantire il rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

Alla domanda deve essere infine allegato un supporto informatico contenente copia del manuale operativo e della dichiarazione tecnica, predisposta utilizzando un sistema di elaborazione testi di larga diffusione.

È data facoltà di non riportare nella dichiarazione tecnica le informazioni soggette a particolari ragioni di riservatezza. Il CNIPA, si riserva, a norma dell'art. 28, comma 5, del testo unico di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato. Il manuale operativo va strutturato in modo tale da essere integralmente consultabile per via telematica, come prescritto dall'art. 38, comma 2, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 e deve contenere, quanto meno, le informazioni previste dal comma 3 dello stesso art. 38. Il piano per la sicurezza, che deve contenere quanto meno le infor-

mazioni di cui all'art. 30 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, deve essere consegnato nel rispetto delle modalità previste nel medesimo articolo.

La domanda e la documentazione da allegare possono essere predisposte, per quanto possibile, in formato elettronico, utilizzando la sottoscrizione con firma digitale e devono poi essere poi inviate alla casella di posta elettronica certificata cnipadir@cert.cnipa.it .

L'istruttoria relativa alle domande e la valutazione della documentazione prodotta sono effettuate dal CNIPA ai sensi del decreto 2 luglio 2004, recante: «Competenza in materia di certificatori di firma elettronica». Al termine dell'istruttoria, il CNIPA, sulla base della documentazione pervenuta, accoglie o rigetta la domanda, ovvero, se necessario, dispone un'integrazione dell'istruttoria.

Nel caso in cui alla domanda non sia allegata tutta la documentazione prevista dalla presente circolare, il richiedente potrà presentare - contestualmente alla domanda stessa – richiesta di sospensione dei termini previsti dall'art. 28, comma 4, del Testo unico.

Il soggetto la cui domanda sia stata oggetto di un provvedimento di reiezione non può presentare una nuova istanza se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente.

Capitolo 16

Bibliografia

G.R. Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings 48 (1979), 313-317.

A. Shamir, How to share a secret, Communications of the ACM 22 (1979), 612-613.