MANUALE OPERATIVO

Certificati Qualificati di Firma Digitale ai sensi del DPR 445/2000, Marcatura Temporale, Carta Nazionale dei Servizi

Il presente documento è stato redatto in coerenza con il Codice Etico e i Principi Generali del Controllo Interno

Dati Identificativi del Documento

Redatto:	*G. Tovo*	.....
Verificato:	*C. Villani*	.....

REGISTRO DELLE MODIFICHE

Versione	Descrizione	Data di Emissione
01.00	Prima Emissione	1 gennaio 2005
01.01	Revisione delle procedure di sospensione e di riattivazione del certificato di firma qualificata, di sostituzione delle chiavi di certificazione del Titolare di FirmaSicura	1 aprile 2005

Sommario

Sommario

Sommario

Sommario

Sommario

PARTE I

Informazioni Generali

1 Scopo del documento

Questo documento illustra le regole generali e le procedure seguite dal Certificatore Accreditato IT Telecom S.R.L. nell'erogazione dei seguenti servizi:

- emissione e gestione di **certificati qualificati di sottoscrizione (Firma Digitale)**. Tali certificati sono identificabili come "qualificati" ai sensi del TUDA, poiché recano al loro interno l'identificativo della Certification Practice Statement (CPS) di riferimento (si veda il par. 1.1 per l'individuazione dell'identificativo della CPS);
- validazione temporale (Time Stamping);
- emissione e gestione di certificati di autenticazione per Carta Nazionale dei Servizi.

Il presente documento:

- è pubblicato a garanzia dell'affidabilità dei servizi del Certificatore nei confronti degli utilizzatori finali e contiene le modalità operative dei servizi indicati;
- costituisce documento pubblico secondo le disposizioni del DPR 28 dicembre 2000, n. 445 e successive modifiche ed integrazioni, nonché della Circolare n. 22 dell'allora AIPA;
- è liberamente disponibile per la consultazione ed il download in formato PDF sul sito predisposto dal Certificatore IT Telecom: http://www.firmasicura.it/manuale-operativo.html, nonché sul sito del CNIPA (http://www.cnipa.it).

1.1 Identificazione della tipologia di certificati emessi

I certificati emessi dal Certificatore I.T. Telecom S.R.L. sono identificabili dalla presenza al loro interno, nel campo policyIdentifier dell'estensione standard certificatePolicies (OID 2.5.29.32), dei seguenti identificativi univoci (OID) registrati presso l'UNINFO:

- Certificati Qualificati di Firma Digitale = 1.3.76.12.1.1.1
- Certificati di Marcatura Temporale = 1.3.76.12.1.1.2
- Certificati di Autenticazione per CNS = 1.3.76.12.1.1.5

I Certificati di Autenticazione per CNS sono ulteriormente identificabili dalla presenza al loro interno, sempre nel campo policyIdentifier suddetto, dell'OID definito dal CNIPA (1.3.76.16.2.1) per indicare l'appartenenza del certificato stesso al circuito della CNS.

2 Identificazione del Certificatore e del Responsabile del Manuale Operativo

La società I.T. Telecom S.R.L., con sede in Milano (MI) – viale Fulvio Testi 250, 20126, esercita l'attività di certificazione della firma qualificata in qualità di **CERTIFICATORE ACCREDITATO** ai sensi del DPR 28 dicembre 2000, n. 445.

Il responsabile del Manuale Operativo è Cinzia Villani, Responsabile dei Servizi di Certificazione Digitale nell'ambito della struttura organizzativa del Certificatore.

3 Riferimenti normativi

Il servizio offerto dal Certificatore è conforme al quadro normativo sintetizzato nella tabella di seguito indicata, nella quale si riportano le abbreviazioni utilizzate nel testo del presente Manuale Operativo per riferimento alle singole norme:

[L. 59/97]	**Legge 15 marzo 1997, n. 59** - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (Gazzetta Ufficiale n. 63 del 17 Marzo 1997, Supplemento ordinario) - Articolo 15, comma 2, relativo alla validità e rilevanza legale degli 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
[TUDA]	**Decreto del Presidente della Repubblica 28 dicembre 2000, n.445** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (GU n. 42 del 20 febbraio 2001) e successive modifiche ed integrazioni, in particolare apportate con il decreto legislativo 23 gennaio 2002, n. 10, con la legge 16 gennaio 2003, n. 3 e il DPR 7 aprile 2003, n.137
[CR22]	**Circolare n. AIPA/CR/22 del 26 luglio 1999** (Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Modalità per presentare domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'art. 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n 513)
[CR24]	**Circolare n. AIPA/CR/24 del 19 giugno 2000** (Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87) – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico dei certificatori di cui all'art. 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n 513)
[DL 10/02]	**Decreto Legislativo 23 gennaio 2002, n. 10** Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale n. 39 del 15 febbraio 2002)
[DL 196/03]	**Decreto Legislativo n. 196 del 30 giugno 2003** - Codice in materia di protezione dei dati personali, pubblicato sul Supplemento ordinario n. 123 della Gazzetta Ufficiale n. 174 del 29 luglio 2003
[DPCM 2004]	**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 (Gazzetta Ufficiale n. 98 del 27 aprile 2004) e successive modifiche ed integrazioni
[DPR 117/04]	**Decreto del Presidente della Repubblica 2 marzo 2004, n. 117** – Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3 (Gazzetta Ufficiale del 6 maggio 2004, serie generale, n. 105)
[LG CNS]	**Linee guida per l'emissione e l'utilizzo della carta nazionale dei servizi** emesse dal CNIPA

4 Standard

I certificati emessi in base al presente documento sono conformi agli standard di riferimento internazionalmente riconosciuti (X509, PKCS, RFC) e a quelli specificamente individuati dalla normativa italiana in materia di Firma Digitale e dalla Commissione Europea secondo la procedura di cui all'art. 9 della Direttiva sopra citata.

In particolare, per quanto concerne i dispositivi di firma si indica il "CWA 14169 (March 2002): Secure Signature-Creation Devices 'EAL 4+'" che definisce i requisiti ai quali deve conformarsi un dispositivo sicuro di firma per l'utilizzo nella firma digitale.

Il sistema qualità del Certificatore è conforme alla norma ISO 9001:2000 per le seguenti attività: Progettazione, realizzazione, erogazione e assistenza di servizi telematici. certificato emesso in data 30 settembre 2003 da CISQ/IMQ-CSQ partner italiano di IQNet. In particolare, per quanto riguarda le attività di sviluppo ed erogazione dei servizi forniti dal Certificatore, si fa riferimento ai processi del Sistema Qualità IT Telecom, relativi alla procedura di sviluppo e alle modalità operative di erogazione dei servizi certificazione digitale.

5 Definizioni, abbreviazioni e termini tecnici

5.1 Definizioni

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale Operativo, i termini e le espressioni sotto elencate avranno il significato descritto nella definizione riportata.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene. Fa eccezione il capitolo 26, nel quale valgono le convenzioni ivi indicate e desunte dal DL 196/03, Codice in materia di protezione dei dati personali.

Si definisce:

Carta di Identità Elettronica (CIE): la carta d'identità elettronica di cui all'articolo 36 del TUDA.

Carta Nazionale dei Servizi (CNS): il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati .

Certificatore *(Certification Authority, CA, Autorità di Certificazione)*: prestatore di servizi di certificazione, la società **I.T. Telecom S.R.L.** Per certificatore, si intende il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

Centro Servizi del Certificatore: La struttura logistica del Certificatore in cui vengono eseguite le principali operazioni relative all'erogazione del servizio di certificazione. Tale struttura è protetta secondo avanzati standard di sicurezza logica e fisica, come dettagliatamente riportato nel Piano per la Sicurezza del Certificatore.

Certificatore Accreditato: È tale***,*** ai sensi dell'art.2, comma 1, lettera c) del DL 10/02, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione Europea ai sensi dell'art. 3, paragrafo 2, della direttiva 1999/93/CE nonché ai sensi del TUDA; **IT Telecom S.R.L.** è un certificatore accreditato in Italia ai sensi del TUDA, che emette, pubblica nel registro e revoca Certificati Qualificati operando in conformità alle regole tecniche e secondo quanto prescritto dal TUDA (art. 1, lett. u e z).

Certificato Qualificato: Un certificato emesso da un certificatore accreditato che risponde ai requisiti di cui all'allegato II della direttiva 1999/93/CE e conforme ai requisiti di cui all'allegato I della medesima direttiva, ai sensi del TUDA e successive modificazioni (art. 1, lett. aa).

Certificazione: Il risultato della procedura informatica applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.

Chiavi asimmetriche: La coppia di chiavi crittografiche una privata e una pubblica, correlate tra loro, e utilizzate nell'ambito dei sistemi di validazione di documenti informatici (art. 22, lett. b) del TUDA).

Chiavi di certificazione: Chiavi asimmetriche utilizzate esclusivamente per apporre la firma su certificati relativi a chiavi di sottoscrizione, di marcatura temporale e di autenticazione per CNS emessi dal

Certificatore, sulle liste dei certificati sospesi e revocati e su nuovi certificati relativi a chiavi di certificazione generate in sostituzione di chiavi scadute.

Chiavi di marcatura temporale: Chiavi asimmetriche utilizzate dal Certificatore per apporre la firma alle marche temporali.

Chiavi di sottoscrizione: Chiavi asimmetriche associate a persone fisiche, da utilizzare per l'apposizione di firme digitali a documenti e ad evidenze informatiche.

Chiave Privata: L'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico (art. 22, lett. c del TUDA).

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 (art. 22, lett. d del TUDA).

Cifratura: La trascrizione di una evidenza informatica secondo un codice riservato che la renda inintelligibile ai terzi. Le operazioni di cifratura e decifrazione si effettuano applicando algoritmi standard che prevedono l'utilizzo di chiavi segrete.

Dati Identificativi del Titolare: il nome, il cognome, il sesso, la data ed il luogo di nascita, il luogo di residenza, il codice fiscale (per quanto riguarda la Carta Nazionale dei Servizi, il luogo di residenza è quello al momento del rilascio della carta stessa).

Dispositivo sicuro per la creazione di una firma: Apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti fissati dalla normativa vigente in materia (art. 1, lett. ii) del TUDA).

Documento informatico: La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. b) del TUDA).

Elenco pubblico dei Certificatori Accreditati: L'elenco pubblico tenuto dal Centro nazionale per l'informatica nella pubblica amministrazione, ai sensi del decreto del Ministro Stanca del 2 luglio 2004.

Estensione del Certificato: Lo standard X.509 versione v3, che definisce i criteri di compilazione dei certificati trattati nel presente Manuale, include la possibilità di inserire nel certificato dati aggiuntivi definiti dal Certificatore (le estensioni del certificato) in aggiunta alle informazioni standard (numero di serie, valore della chiave pubblica, periodo di validità, ecc.).

Evidenza informatica: Una sequenza di simboli binari che può essere elaborata da una procedura informatica.

Firma di un documento o di una evidenza informatica: Il processo informatico attraverso cui l'impronta di un documento o di una evidenza informatica è cifrata con la chiave privata del firmatario, secondo modalità che consentano al destinatario di verificare la provenienza e l'integrità del documento tramite la chiave pubblica ed il relativo certificato.

Firma digitale: Un particolare tipo di firma elettronica qualificata, basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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 (art. 1, lett. n del TUDA).

Firma elettronica: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

Firma elettronica avanzata: firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, 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;

Firma elettronica qualificata: firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.

Funzione di hash: Una funzione matematica che,da una generica sequenza di simboli binari di partenza, genera una sequenza di simboli binari derivata (detta impronta). La sequenza derivata è generata in modo tale che non sia possibile risalire alla sequenza di partenza e che, a fronte di sequenze di partenza diverse, non possano essere generate sequenze derivate identiche.

Impronta di un documento o di una evidenza informatica: sequenza di simboli binari, di lunghezza predefinita, generata mediante l'applicazione di una opportuna funzione di hash al documento.

Indice Nazionale delle Anagrafi (INA): il sistema del Ministero dell'Interno, Centro nazionale per i servizi demografici di cui all'articolo 2-quater del decreto-legge 27 dicembre 2000, n. 392, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 26. L'INA contiene, per ogni cittadino residente in Italia, le informazioni seguenti (validate dal Comune per la parte anagrafica e la residenza e dall'Agenziadelle Entrate per quanto riguarda il codice fiscale): codice fiscale, cognome, nome, sesso, data di nascita, codice del comune di nascita, codice del comune di residenza, data di eventuale decesso.

Lista dei Certificati Revocati e Sospesi o Lista di Revoca/Sospensione - (Certificate Revocation/Suspension List o CRL/CSL): La lista firmata digitalmente, tenuta e aggiornata dal certificatore, dei certificati che hanno perduto temporaneamente (sospesi) o definitivamente (revocati) la propria validità, in anticipo rispetto alla scadenza prevista.

La revoca e la sospensione, che possono essere richieste dai titolari dei certificati, dal Certificatore o da terzi interessati, o disposte su iniziativa del Certificatore, determinano l'inserimento del certificato nella lista dei certificati revocati e sospesi.

La lista è resa pubblica tramite il Registro dei Certificati del Certificatore.

I motivi che possono portare alla revoca o sospensione di un certificato e le modalità di revoca e sospensione sono riportati nel seguito del presente Manuale.

Lista di revoca della CNS:, è costituita dagli elenchi delle CNS che sono state segnalate all'Indice Nazionale delle Anagrafi come emesse e che sono revocate dalle amministrazioni emittenti.

Marca temporale: Un'evidenza informatica che consente la validazione temporale.

Manuale Operativo: Il documento pubblico che definisce le modalità operative del servizio di certificazione (art. 38 del DPCM 2004).

Manuale della Qualità: Il manuale predisposto dal Certificatore per ottenere la certificazione di qualità ISO 9002, come previsto dalla normativa vigente.

Piano per la Sicurezza: Il documento, previsto dal DPCM 2004 e conforme al TUDA, che definisce le modalità di gestione delle attività connesse alla protezione e conservazione di dati, programmi ed apparati del Certificatore. Tale documento, che contiene informazioni riservate, non è divulgato pubblicamente ma depositato presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, a garanzia della sua completezza e conformità a quanto previsto dalla normativa vigente e dagli attuali standard internazionali di sicurezza (art. 30 del DPCM 2004).

Pubbliche Amministrazioni: le amministrazioni di cui all'articolo 1, comma 2, ed all'articolo 70, comma 4, del decreto legislativo 30 marzo 2001, n. 165.

Registro dei Certificati (Directory): Un archivio pubblico, in formato elettronico, consultabile da chiunque 24 ore su 24, dotato di requisiti di sicurezza e affidabilità tali da garantire l'autenticità, l'integrità e la disponibilità dei dati in esso contenuti.

Registrazione di un utente, un sottoscrittore, un titolare: La procedura che precede il rilascio di un certificato da parte del Certificatore e che prevede l'acquisizione dei dati identificativi del titolare.

Revoca di un Certificato: L'operazione mediante la quale il Certificatore annulla in maniera irreversibile, su iniziativa propria o del titolare o di terze parti interessate, la validità del certificato da un dato momento in poi (art. 22, lett. l del DPCM 2004).

Sistema biometrico di autenticazione: Apparecchiatura per l'autenticazione dell'identità di un individuo attraverso la misurazione o analisi di caratteristiche del corpo umano quali impronte digitali, retina, iride, sequenze vocali, morfologia del viso, o altro.

Smartcard: Dispositivo elettronico costituito da un microchip inserito in una tessera in plastica delle dimensioni di una carta di credito. Il microchip è programmabile, può contenere dati e applicativi e interagire con altre apparecchiature elettroniche e computer tramite un apposito lettore.

Sospensione di un certificato: L'operazione con cui il Certificatore sospende la validità del certificato per un determinato periodo di tempo (art. 22, lett. m del DPCM 2004).

Titolare: è la persona fisica cui é attribuita la firma elettronica e che ha accesso al dispositivo per la creazione della firma elettronica (art. 1 lett. ff) del TUDA). Detiene una chiave privata per l'apposizione di firme digitali ed è intestataria del certificato che attesta il valore della chiave pubblica ad essa relativa. Il titolare può utilizzare la chiave privata e il certificato per apporre firme digitali come privato, o in base al

proprio ruolo all'interno di un'organizzazione pubblica o privata, ovvero in base a poteri di rappresentanza o titoli e abilitazioni professionali.

5.2 Abbreviazioni e termini tecnici

AIPA - Autorità per l'Informatica nella Pubblica Amministrazione: Autorità pubblica indipendente, istituita dal decreto legislativo n. 39 del 12 febbraio 1993 "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche" (come modificato dall'art.42 della legge 31 dicembre 1996, n.675). L'AIPA ha cambiato denominazione in CNIPA con l'articolo 176 del DL 196/003.

CC - Common Criteria: Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), americani (Federal Criteria), e canadesi (Canadian Criteria).

CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione: creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico

DNS - Domain Name System: Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti Internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.telecomitalia.it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3). Con il termine DNS si intendono, per estensione, anche le sequenze numeriche convenzionali che identificano i domini.

Regole Tecniche (oppure DPCM 2004): Il riferimento normativo è al DPCM 13 gennaio 2004, che riporta le "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 8, comma 2, del TUDA.

HTTP (Hypertext Transfer Protocol): Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web.

HTTPS (Secure Hypertext Transfer Protocol): Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifrazione dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad una estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.

INTERNET: Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW).

ISO - International Standards Organization: Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO.

ITSEC - Information Technology Security Evaluation Criteria: Criteri europei per la valutazione della sicurezza nei sistemi informatici.

ITU - International Telecommunication Union: Organizzazione internazionale che funge da ente regolatore per gli standard nelle telecomunicazioni.

ITU – T: Sigla identificativa del Settore Telecomunicazioni ("Telecommunication Sector") dell'ITU.

LDAP – Lightweight Directory Access Protocol: Protocollo utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.

OID - Object identifier: Sequenza numerica che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO.

PIN - Personal Identification Number: Codice di sicurezza riservato che permette l'attivazione delle funzioni del dispositivo di firma.

POP – Point of Presence: Punto di accesso alla rete Internet.

PKCS - Public Key Cryptography Standard: Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.

PKI – Public Key Infrastructure: Infrastruttura informatica costituita da applicazioni che utilizzano tecniche crittografiche a chiave pubblica. Un'infrastruttura a chiave pubblica include servizi di generazione e

distribuzione di chiavi, emissione e pubblicazione di certificati, gestione dei registri dei certificati emessi e delle liste di sospensione e revoca, altri servizi come l'emissione di marche temporali. Esempi di funzionalità basate sull'infrastruttura sono: la generazione di transazioni informatiche riservate (crittografia), la gestione di sistemi di autorizzazione, autenticazione e identificazione (firma digitale), riferibilità soggettiva ed integrità dei dati (firma digitale e marcatura temporale).

RFC – Request for Comments: Definizioni scritte di protocolli o standard in uso su Internet.

SL - Secure Socket Layer: Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.

URL - Uniform Resource Locator: Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica le modalità di accesso all'oggetto.

WWW – World Wide Web: L'insieme delle risorse e degli utenti su Internet che utilizzano il protocollo HTTP.

X509: Specifica ITU-T che definisce la struttura e la terminologia da utilizzare per la compilazione dei certificati e delle liste ad essi associate.

6 Natura dei servizi

6.1 Servizio di Certificazione della Firma Digitale

L'emissione di certificati qualificati di sottoscrizione, fa riferimento alla firma digitale, un servizio finalizzato ad assicurare la **paternità ed integrità** ai documenti informatici elaborati e/o sottoscritti da un soggetto mediante la fornitura di specifici dispositivi hardware e software.

La firma digitale è basata su un procedimento di "crittografia asimmetrica", che fa uso di una coppia di chiavi asimmetriche di lunghezza pari ad almeno 1024 bit: una privata, utilizzata per firmare (da tenersi, di norma, segreta e conservata in maniera sicura dal titolare), e una pubblica, utilizzata per le operazioni di verifica della firma. La corrispondenza tra le chiavi di firma e il sottoscrittore è garantita da un Certificatore (terza parte fidata) riconosciuto dal CNIPA .

Per meglio distinguere il diverso profilo degli utenti del servizio di Certificazione della Firma Digitale si identificano gli attori principali:

- **Gestore del servizio/Terza Parte Fidata**: il Certificatore che garantisce, mediante l'emissione del certificato digitale, l'associazione tra la persona (Titolare) e la sua chiave pubblica (e quindi anche alla corrispondente chiave privata), generata all'interno del dispositivo sicuro di firma.
- **Cliente**: il soggetto che sigla il contratto di fornitura con il Certificatore, relativo alla fornitura del servizio di Certificazione in favore dei soggetti richiedenti afferenti alla propria organizzazione. Nel caso di richiedente a titolo personale, il cliente ed il titolare coincidono..
- **Titolari**: i soggetti che possono utilizzare il certificato di firma digitale per firmare documenti informatici, che assumono così la rilevanza giuridica dettata dalla normativa in materia.
- Il Certificatore prevede la possibilità di demandare l'attività di identificazione e registrazione dei titolari ad Incaricati identificati nell'ambito dell'organizzazione del cliente quando questi appartenga alla Pubblica Amministrazione. In questo caso, sono previsti **Incaricati dell'Identificazione dei Titolari e della consegna dei dispositivi di firma**,ovvero dipendenti del Cliente incaricati congiuntamente dal Certificatore e dal Cliente ad effettuare le operazioni di identificazione e di registrazione (v. par. 10.2 e cap. 12) degli utenti titolari appartenenti all'ente richiedente. Tali soggetti fungono da punto di riferimento interno all'Amministrazione per i rapporti tra il certificatore ed i titolari e consegnano loro i kit del servizio.

Gli Incaricati sono muniti di idonei strumenti per l'accesso all'applicativo web che consente di automatizzare le operazioni di registrazione dei Titolari (smartcard con certificato di autenticazione o identificativo personale e password).

I Titolari del servizio, dispongono di un dispositivo sicuro di firma nel quale è stata generata una coppia di chiavi assieme ad un certificato di firma che consente l'associazione della persona con la sua chiave pubblica. Tale associazione avviene solo dopo l'identificazione e la registrazione certa del richiedente da

parte del Certificatore che ha anche il compito di gestire l'intero ciclo di vita del certificato compresa la sospensione temporanea della sua validità o la sua revoca definitiva.

Al Titolare viene consegnato un kit composto da un insieme di prodotti e viene assicurata la fornitura di tutti i servizi accessori:

- Generazione di una coppia di chiavi di lunghezza pari ad almeno 1024 bit;
- Emissione e gestione del certificato qualificato di Firma Digitale, come definito dalla vigente normativa sulla documentazione amministrativa (TUDA e successive modifiche) e gestito secondo le norme di qualità (UNI EN ISO 9002);
- Fornitura del dispositivo sicuro di firma contenente il Certificato di Firma Digitale;
- Fornitura del lettore di smartcard (ove necessario);
- Fornitura dell'applicativo client (software) per la firma, la verifica delle firme ed eventualmente per la cifratura dei documenti (dispositivo di verifica della firma);
- Fornitura della manualistica di supporto;
- Servizio di Registrazione dei Titolari;
- Servizio di help desk per l'assistenza in fase di installazione dei dispositivi HW e SW e l'inoltro delle richieste di sospensione, riabilitazione e revoca del certificato.

6.2 Servizio di Marcatura Temporale

Il servizio di Validazione Temporale del Certificatore permette di attribuire ad uno o più documenti informatici un **riferimento temporale opponibile ai terzi**, costituito da una data ed un'ora certe asseverate mediante la generazione di una marca temporale.

Ciascuna marca generata ed apposta su un documento informatico è indissolubilmente legata al documento stesso grazie a riferimenti certi (impronta del documento, numero progressivo seriale, identificativo della CA). Con l'associazione di un riferimento temporale ai propri documenti elettronici l'utente può dimostrare la loro esistenza ad un determinato istante e dare loro la validità legale corrispondente alla tipologia di firma utilizzata per la sottoscrizione.

6.3 Carta Nazionale dei Servizi

Le carte utilizzate per l'accesso ai servizi in rete erogati dalla Pubblica Amministrazione sono costituite da diverse tipologie di smartcard che hanno in comune le seguenti caratteristiche:

- sono **emesse da un ente pubblico** che convalida le informazioni di rilevanza sociale in esse contenute;
- hanno **requisiti di sicurezza** che permettono di utilizzare in rete queste informazioni con la massima garanzia di sicurezza.

Le carte per l'accesso ai servizi sono riconducibili a due tipologie:

- la **Carta d'Identità Elettronica (CIE)**, emessa dai Comuni in sostituzione della carta d'identità tradizionale;
- gli altri dispositivi di autenticazione per accedere ai servizi in rete (carta sanitaria, carta nazionale dei servizi, carta tributaria, carte regionali e cittadine dei servizi, ecc.), che devono essere conformi a un unico **standard** denominato "**Carta Nazionale dei Servizi**" **(CNS)**.

La CNS, dunque, è strumento di identificazione in rete basato su una carta a microprocessore in grado di gestire procedimenti di crittografia asimmetrica, che presenta le stesse caratteristiche funzionali della CIE, ma non contiene gli elementi "esterni" tipici di una carta d'identità (ad esempio, la fotografia). La CNS consente anche l'inserimento delle informazioni relative alla firma digitale, allo scopo di consentire ai titolari di sottoscrivere documenti elettronici.

Nel processo di emissione e gestione della CNS, la normativa vigente individua i seguenti attori, con i rispettivi ruoli:

- **Ente Emettitore**: l'ente della Pubblica Amministrazione che emette la CNS. Le sue responsabilità sono relative a:

  - correttezza dei dati identificativi e del codice fiscale del titolare memorizzati nella carta e nel certificato di autenticazione;
  - sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta;
  - invio dei dati identificativi al Ministero dell'Interno (INA).
- **Produttore delle carte**: l'azienda che provvede alla fornitura delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, per la quale
  - predispone opportunamente gli spazi dedicati alla carta sanitaria (Netlink) ed alla firma digitale;
  - applica al supporto fisico l'artwork (aspetto grafico esterno) e gli elementi costanti.
- **Certificatore**: il soggetto che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche (sono abilitati a prestare tali servizi per la CNS i soggetti di cui all'articolo 5 del DL 10/02).
- **Distributore delle carte**: è il soggetto che distribuisce le carte opportunamente predisposte dal produttore delle carte e dal certificatore in base ai dati forniti dall'ente emettitore.
- **Titolari**: il cittadino che possiede la CNS e che la può utilizzare per l'accesso ai servizi in rete.

7 Destinatari e tariffe dei servizi

La distribuzione sul mercato dei servizi indicati nel presente Manuale Operativo è effettuata da IT Telecom S.R.L. e dalle strutture commerciali dell'azienda Telecom Italia.

7.1 Certificazione della Firma Digitale

I destinatari dell'offerta commerciale comprendente l'emissione e la gestione dei certificati relativi a chiavi di sottoscrizione sono:

- Enti, aziende, istituti ed altri soggetti appartenenti alla Pubblica Amministrazione;
- Persone giuridiche che intendono far utilizzare il servizio alle persone fisiche ad esse direttamente afferenti. Tali persone fisiche costituiscono i Titolari dei certificati, ovverosia gli utenti finali del servizio;
- Persone fisiche, a titolo privato;

Parte dei livelli di servizio garantiti per l'insieme delle attività inerenti l'emissione di certificati relativi a chiavi di sottoscrizione ed autenticazione e dei corrispondenti dispositivi, quali ad esempio i tempi di consegna, sono definiti nell'ambito degli specifici contratti stipulati con l'acquirente dei certificati.

Il solo servizio, come descritto nel presente documento, è fornito alle seguenti condizioni economiche:

- canone annuale di € 50, per l'emissione e la gestione del Certificato Qualificato;
- € 50 per ciascuna sospensione e ciascuna riabilitazione richieste per il Certificato Qualificato, con la sola esclusione della sospensione preventiva alla revoca (v. par. 15.3.1);
- sono esclusi gli accessori (dispositivo sicuro di firma, lettore del dispositivo, ecc.).

Dette condizioni sono da ritenersi indicative, in quanto soggette all'andamento del mercato e variabili in funzione delle quantità richieste.

7.2 Marcatura Temporale

I destinatari dell'offerta commerciale relativa all'emissione di marche temporali sono gli stessi individuati al precedente paragrafo.

Parte dei livelli di servizio garantiti per l'insieme delle attività inerenti l'emissione delle marche temporali, sono definiti nell'ambito degli specifici contratti stipulati con l'acquirente del servizio.

7.3 Carta Nazionale dei Servizi

I destinatari dell'offerta commerciale inerente la Carta Nazionale dei Servizi sono le Pubbliche Amministrazioni aventi titolo all'emissione e alla gestione delle CNS per i propri utenti e che agiscono in qualità di Enti Emettitori.

Il servizio è fornito agli Enti Emettitori con le modalità descritte nel capitolo 24.2, in funzione delle richieste effettuate dagli stessi.

8 Ambito di applicazione

Le **coppie di chiavi generate** dal certificatore per i servizi ad esse correlate sono le seguenti (art. 4, comma 4 del DPCM 2004):

- **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 ai certificati relativi a chiavi di marcatura temporale;
- **chiavi di sottoscrizione**, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
- **chiavi di marcatura temporale**, destinate alla generazione e verifica delle firme apposte alle marche temporali.

Al di fuori dell'ambito definito dal DPCM 2004, il Certificatore genera inoltre coppie di chiavi di autenticazione, destinate alla generazione e verifica delle firme apposte ai certificati utilizzati nell'ambito dei servizi per CNS.

Le applicazioni relative alle tipologie di certificati emessi sono le seguenti:

- **Certificati relativi a chiavi di certificazione:** sono utilizzati esclusivamente per apporre la firma sui certificati relativi a chiavi di sottoscrizione e di marcatura temporale emessi dal Certificatore, sulle liste dei certificati sospesi e revocati e su nuovi certificati relativi a chiavi di certificazione emesse in sostituzione di analoghe chiavi scadute;
- **Certificati relativi a chiavi di sottoscrizione:** sono i certificati relativi alle chiavi associate a persone fisiche, utilizzati per l'apposizione di firme digitali a documenti ed evidenze informatiche;
- **Certificati relativi a chiavi di marcatura temporale:** sono utilizzati per apporre la firma alle marche temporali emesse.

9 Cenni sulle infrastrutture del Certificatore

La generazione dei certificati qualificati avviene su un sistema utilizzato esclusivamente per la generazione di certificati, situato in locali adeguatamente protetti (art. 28 comma 1 del DPCM 2004), per il quale qui di seguito si indicano gli aspetti più rilevanti:

- La piattaforma è stata progettata in modo da garantire nel tempo la capacità di incrementare gradualmente nel tempo la **performance** e la **capacità di produzione** attraverso l'espansione dello spazio disco utilizzabile e l'aggiunta di ulteriori sistemi di emissione certificati. Pertanto l'infrastruttura di erogazione si caratterizza per la sua **flessibilità** e garantisce l'adeguamento fino al livello massimo di produzione, dai singoli certificati ai lotti di grandi dimensioni.
- La piattaforma di erogazione adotta **soluzioni hardware e software leader di mercato** per interoperabilità, affidabilità e sicurezza:
  - software di PKI certificato per il software core di CA rispetto ai Common Criteria (CC) (EAL3) ed a al FIPS PUB 140-1;
  - dispositivi crittografici (Hardware Security Module, HSM) per la gestione delle chiavi di certificazione certificati FIPS PUB 140-1 level 4.
- Per ciascuna delle tipologie di servizio indicate nel presente Manuale Operativo, sono utilizzate Certification Authority dedicate.
- La continuità del servizio di gestione dei certificati è garantita grazie a sistemi di **disaster recovery** e di **ridondanza funzionale**.

- IT Telecom dispone di un pool di risorse con uno specifico know-how sulle tecnologie del mondo dei certificati digitali e delle strutture di PKI, continuamente aggiornato attraverso attività di scouting e di contatto con i principali vendor del settore. Il Competence Center IT Telecom può vantare una collaborazione pluriennale con il CNIPA (ex AIPA e Centro Tecnico RUPA) e con altri enti italiani e stranieri (Assocertificatori, ecc.) ed è a disposizione dei clienti che necessitano di un supporto tecnico e consulenziale per risolvere tutte le problematiche relative alla progettazione dei servizi, alla definizione delle policy di gestione, al disegno delle architetture ed al relativo project management.

L'infrastruttura per l'erogazione dei servizi del certificatore è organizzata logicamente su cinque componenti:

- Il **Sistema di Autenticazione** provvede all'autenticazione dei soggetti che accedono al servizio, gestita tramite policy configurabili. Ogni componente della struttura è ridondato e configurato per garantire elevati livelli di sicurezza e riservatezza dei dati per ogni singolo cliente.
- La **Componente di Front-End** realizza tutte le funzionalità necessarie alla gestione delle smartcard e del ciclo di vita dei certificati; esposta su Internet/Intranet, è l'unica componente autorizzata a colloquiare con la componente di Back-End posta nella zona protetta;
- La **Componente di Back-End** è inserita nella zona più protetta della rete del Certificatore IT Telecom e non viene esposta all'esterno (ossia non è per nessuna ragione raggiungibile direttamente da Internet), fornisce le funzionalità fondamentali della PKI e dei servizi del Certificatore (Posta Certificata, Time Stamping Authority , Authentication Server ecc..);
- La **Rete di Gestione** permette agli operatori del Certificatore di raggiungere i sistemi posti sulle reti di Front End e Back End per le attività di gestione. Tale rete è posta all'interno della Sala Sistemi del Centro Servizi del Certificatore e non è raggiungibile dall'esterno. I collegamenti sono effettuati in modalità SSH con accesso controllato da FIREWALL e autenticazione centralizzata LDAP. Le reti di Front End e di Back End sono protette da sistemi FIREWALL in configurazione di High Availability;
- **Rete di backup**: garantisce il servizio di salvataggio ed archiviazione dei dati.

Fra le principali **misure di sicurezza** che vengono adottate per garantire che le attività del Certificatore si svolgano secondo i requisiti di sicurezza richiesti dalla normativa vigente, si ricordano:

- I meccanismi per il controllo dell'accesso logico e fisico alle risorse e ai sistemi del Certificatore, che forniscono le seguenti funzionalità:
  - identificano ed autenticano le persone autorizzate ad accedere alle risorse;
  - impediscono ad una persona non autorizzata di poter accedere alle risorse;
  - registrano i dati significativi di tutti gli eventi di accesso in modo che si possa in ogni caso risalire alla persona che ha dato origine ad un determinato evento.
- Il controllo dell'accesso ai locali protetti adotta una politica di autorizzazioni e di procedure di registrazione e auditing.
- L'accesso alla Sala Sistemi del Centro Servizi del Certificatore è basata sul principio secondo il quale nessuno da solo è autorizzato ad accedere alle risorse presenti nel locale: ogni persona che intende accedere alle risorse della Sala Sistemi è identificata in modo certo, mediante l'utilizzo di una smartcard o un token personale.
- In particolare, l'avvio e la conclusione di ciascuna sessione di lavoro del sistema di generazione dei certificati qualificati è registrata sul giornale di controllo.

Le caratteristiche di dettaglio della gestione della sicurezza del certificatore sono contenute nel **Piano della Sicurezza** e non sono oggetto di divulgazione, per salvaguardarne l'efficacia.

PARTE II

Condizioni di utilizzo del servizio di certificazione della firma digitale

10 Obblighi, Responsabilità e Indennizzi

Questo capitolo definisce gli obblighi e le relative responsabilità del Certificatore, del richiedente la certificazione, del titolare del certificato, del terzo interessato di cui all'art. 28 comma 2 del TUDA e di quanti accedono al registro dei certificati per la verifica delle firme, nonché le eventuali limitazioni agli indennizzi che possono essere richiesti al Certificatore.

Per ciò che non è espressamente stabilito nel presente capitolo, varrà, in relazione a ciascuno dei soggetti volta a volta coinvolti, quanto previsto dalle disposizioni normative applicabili e, in particolare, dal TUDA nonché dal DPCM 2004 e loro eventuali successive modificazioni ed integrazioni.

10.1 Obblighi del Certificatore

Il Prestatore di Servizi di Certificazione è tenuto ad attenersi quanto stabilito dal TUDA e dal DPCM 2004. In particolare:

- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 29 bis, comma 1 del TUDA);
- **identificare con certezza** la persona che fa richiesta del servizio di certificazione (art. 29 bis, comma 2, lett. a del TUDA);
- **rilasciare e rendere pubblico il certificato** elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'art. 8, comma 2 del DPR445/00 (art. 29 bis, comma 2, lett. b del TUDA) e nel rispetto del DL 196/03;
- **verificare che la chiave pubblica della quale si richiede la certificazione non sia già stata certificata**, per un altro soggetto titolare, nell'ambito del proprio dominio.;
- 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 sussistenza degli stessi; (art. 29 bis, comma 2, lett. c del TUDA);
- 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 (art. 29 bis, comma 2, lett. e del TUDA);
- adottare le misure di sicurezza per il **trattamento dei dati personali**;
- non rendersi depositario di dati per la creazione della firma del titolare (art. 29 bis, comma 2, lett. g del TUDA);
- procedere alla 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 di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni (art. 29 bis, comma 2, lett. h del TUDA);
- garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo (art. 29 bis, comma 2, lett. i del TUDA);
- assicurare la **precisa determinazione** della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici (art. 29 bis, comma 2, lett. l del TUDA);
- tenere **registrazione**, anche elettronica, di tutte le informazioni relative al certificato per **almeno dieci anni dalla data di scadenza del certificato**, in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari (art. 29 bis, comma 2, lett. m del TUDA);
- **non copiare né conservare le chiavi private di firma** del soggetto cui il certificatore ha fornito il servizio di certificazione, né i dispositivi di firma che le contengono (art. 29 bis, comma 2, lett. n del TUDA e art. 7, comma 1 del DPCM 2004);
- 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 e il certificatore (art. 29 bis, comma 2, lett. o del TUDA);

- 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 alle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato (art. 29 bis, comma 2, lett. p del TUDA);
- indicare o rilasciare un **dispositivo sicuro per la generazione delle firme**, che presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 29-sexies del TUDA e all'art. 9 del DPCM 2004;
- fornire ovvero indicare almeno un **sistema che consenta di effettuare la verifica delle firme digitali** (art. 10 del DPCM 2004) e garantire l'interoperabilità del prodotto di verifica per i documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative (art. 40, comma 2 del DPCM 2004).

10.1.1 Utilizzo delle chiavi in relazione alla loro diversa tipologia

Il Certificatore utilizza le diverse chiavi di cui è titolare esclusivamente per le funzioni previste dalla rispettiva tipologia (art. 4, comma 5 del DPCM 2004).

10.1.2 Polizza assicurativa

Il Certificatore è dotato di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi (art. 11, comma 1, lett. m del DPCM 2004), con le seguenti caratteristiche:

Tipo di Risarcimento	Massimale annuo	Massimale per singolo sinistro
Risarcimento di danni patrimoniali cagionati a Terzi in conseguenza di fatto accidentale verificatosi in relazione allo svolgimento dell'attività del certificatore , oppure per fatto doloso dei dipendenti addetti all'attività per la quale è prestata l'assicurazione e dei quali il Certificatore debba rispondere ai sensi di legge	€ 1.548.370,70	€ 258.228,45
Risarcimento per danni conseguenti alla diffusione di dati personali della persona fisica, giuridica, ente o associazione, che sia avvenuta involontariamente o per infedeltà del personale autorizzato, dipendente o non, dal Certificatore.	€ 516.456,90	€ 258.228,45

10.2 Obblighi associati all'attività di Identificazione e Registrazione dei Richiedenti e dei Titolari

L'attività di Identificazione e Registrazione dei Titolari e dei richiedenti è svolta dal Certificatore in modalità diretta o delegata attraverso soggetti incaricati dell'identificazione dei titolari e della consegna dei dispositivi di firma[1]. Sia il Certificatore sia gli Incaricati dell'Identificazione sono tenuti a:

- Identificare con certezza il richiedente del servizio di certificazione (art. 29 bis, comma 2, lett. a del TUDA);
- Informare espressamente il richiedente la registrazione riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza e alla conservazione della chiave privata nonché all'uso dei dispositivi di firma;
- Fornire al richiedente tutte le informazioni attinenti il trattamento dei suoi dati personali in ottemperanza a quanto previsto dal DL 196/03.
- Far firmare, su modulo cartaceo, la richiesta di adesione al servizio di Certificazione;

In particolare, gli **Incaricati dell'Identificazione dei Titolari e della consegna dei dispositivi di firma** (v. par. 6.1) sono tenuti a:

[1] Gli Incaricati dell'Identificazione, ove non appartenenti all'organizzazione del Certificatore, sono da questo identificati con procedura analoga a quella prevista per l'identificazione dei richiedenti.

- Comunicare e trasmettere al Certificatore tutti i dati e i documenti acquisiti durante la registrazione del titolare allo scopo di attivare la procedura di emissione del certificato. Il Certificatore conserva detta documentazione per un periodo non inferiore a dieci anni dalla data di scadenza del certificato che sarà emesso a seguito della richiesta di registrazione (art. 29 bis, comma 2, lett. m del TUDA);
- Verificare e inoltrare al Certificatore le richieste di revoca o sospensione nel caso di procedura attivata dall'utente titolare.

10.3 Obblighi associati all'attività di consegna dei dispositivi sicuri di firma e dei codici segreti per l'utilizzo del servizio

L'attività di consegna ai Titolari dei dispositivi sicuri di firma e dei codici segreti per l'utilizzo dei servizi è svolta dal Certificatore in modalità diretta o delegata attraverso gli Incaricati dell'Identificazione dei Titolari e della consegna dei dispositivi di firma. Chiunque dei soggetti indicati effettui la consegna è tenuto a:

- Assicurarsi che chi ritira i dispostivi ed i codici segreti sia effettivamente il Titolare che ha richiesto l'emissione del certificato.
- *Assicurarsi che al richiedente siano state fornite tutte le informazioni attinenti il trattamento dei suoi dati personali in ottemperanza a quanto previsto dal DL 196/03.*
- Far firmare al Titolare, su modulo cartaceo, la dichiarazione mediante la quale attesta di aver ricevuto il dispositivo sicuro di firma;
- Far firmare al Titolare, su modulo cartaceo, la dichiarazione mediante la quale attesta di aver ricevuto i codici segreti e che questi gli sono stati consegnati in un involucro che non presentava nessun segno evidente di effrazione;
- Trasmettere al Certificatore i documenti acquisiti durante la consegna dei dispositivi di firma e dei codici segreti.

10.4 Obblighi del richiedente e del titolare

Il titolare e il richiedente sono tenuti ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 29 bis, comma 1 del TUDA). Il richiedente e il titolare della chiave devono inoltre:

- **Consultare preventivamente il presente Manuale Operativo** e conoscerne i contenuti. Il Certificatore non sarà responsabile di eventuali danni o pregiudizi nella misura in cui tali danni e pregiudizi avrebbero potuto essere evitati o limitati dalla conoscenza delle previsioni contenute nel presente Manuale.
- **Inoltrare richiesta di registrazione al Certificatore** direttamente o tramite l'Incaricato per l'identificazione e la consegna dei dispositivi di firma, secondo le modalità indicate nel capitolo 12 del presente Manuale Operativo.
- **Fornire tutte le informazioni e la documentazione richieste dal Certificatore** o dall'Incaricato per l'identificazione e la consegna dei dispositivi di firma, necessarie ad una corretta identificazione personale garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del TUDA.
- Comunicare al Certificatore o all'Incaricato dell'Identificazione, l'eventuale **variazione di residenza e di tutti i dati previsti** al punto precedente anche dopo l'emissione del certificato.
- **Indicare al Certificatore o all'Incaricato dell'Identificazione, eventuali limitazioni nell'uso della coppia di chiavi** (art. 27 bis, comma 3, lett. b e c del TUDA e art. 43 del DPCM 2004), eventuali poteri di rappresentanza e abilitazioni professionali (art 27 bis, comma 3, lett. a del TUDA), presentando al certificatore idonea documentazione giustificativa.
- Far sì che l'eventuale generazione della coppia di chiavi di sottoscrizione da parte del titolare, ove prevista e consentita dal presente Manuale Operativo, **avvenga all'interno del dispositivo di firma**, nel rispetto delle norme e delle modalità tecniche al riguardo previste dalla vigente normativa (art. 6 commi 3 e 4 del DPCM 2004).
- Indicare esplicitamente e per iscritto, nella richiesta di certificazione di una coppia di chiavi, tutte le **informazioni che non desiderano che siano inserite nel certificato**, ad esclusione di quelle considerate obbligatorie ai sensi di legge. Il Certificatore non sarà pertanto responsabile nei confronti del titolare per l'inserimento nel certificato, nel rispetto delle vigenti norme di legge, di informazioni non esplicitamente escluse per iscritto dal titolare.

- Attenersi a tutte le disposizioni del DPCM 2004 che li riguardano, in particolare **il Titolare ha l'obbligo di**:
  - ✓ Utilizzare esclusivamente il dispositivo fornito dal certificatore ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso (art. 6, comma 5 del DPCM 2004).
  - ✓ Conservare le chiavi private all'interno del dispositivo di firma.
  - ✓ Conservare con la massima diligenza la propria chiave privata ed il dispositivo di firma che la contiene al fine di preservarne l'integrità e la riservatezza (art. 7, comma 3, lett. a del DPCM 2004).
  - ✓ Conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso da quello in cui è conservato il dispositivo contenente la chiave (art. 7, comma 3, lett. b del DPCM 2004).
  - ✓ Richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso (art. 7, comma 3, lett. c del DPCM 2004).
  - ✓ Sottoscrivere la richiesta di revoca specificandone la motivazione e la sua decorrenza (art. 19 commi 1 e 2 del DPCM 2004).
  - ✓ Sottoscrivere la richiesta di sospensione specificando la motivazione e il periodo durante il quale la validità del certificato deve essere sospesa (art. 23, comma 1 e 2 del DPCM 2004).
  - ✓ Notificare l'eventuale compromissione della chiave privata.
  - ✓ Verificare che il dispositivo di firma di cui si avvale proceda all'identificazione del titolare stesso prima di generare la firma digitale.
  - ✓ Utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso, se appone la propria firma per mezzo di una procedura automatica. Inoltre, 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 (art. 4, commi 2 e 3 del DPCM 2004).
  - ✓ Controllo lo stato del certificato prima di generare la firma digitale, attenendosi alle modalità previste nel successivo paragrafo 10.5 (art. 23, comma 2 del TUDA).
  - ✓ In caso di attribuzione di più codici identificativi distinti per ciascuno dei ruoli per cui può firmare, utilizzare ciascun codice esclusivamente in relazione al ruolo per il quale esso è stato attribuito; **il Certificatore non è responsabile di qualsiasi pregiudizio, diretto od indiretto, derivante dall'erroneo utilizzo dei codici identificativi da parte del titolare**.
  - ✓ In caso di assenza o impossibilità di utilizzare il sistema di comunicazione sicuro con il Certificatore o gli altri sistemi di comunicazione previsti nel presente Manuale Operativo, effettuare le comunicazioni al Certificatore presso la sede del Certificatore medesimo o altro ufficio appositamente indicato dal Certificatore.
  - ✓ **Non duplicare** la propria chiave privata ed i dispositivi che la contengono (art. 7, comma 1 del DPCM 2004).
  - ✓ Corrispondere al Certificatore quanto previsto a proprio carico.

10.4.1 Consenso e informazioni dovute dal terzo interessato

Al fine dell'indicazione nel Certificato del titolare delle informazioni previste dall'Art.27 bis, comma 3, del TUDA, al terzo interessato è fatto onere di prestare il proprio consenso in conformità a quanto previsto nei paragrafi 12.1.1, 12.1.2 e 12.1.3 del presente Manuale Operativo, fornendo, a richiesta del Certificatore, tutti i documenti e le informazioni allo scopo necessarie. L'interessato, inoltre, deve informare tempestivamente il Certificatore di ogni eventuale modificazione delle informazioni e dei dati forniti ed è responsabile della loro veridicità, completezza ed attualità.

10.5 Obblighi di chi accede per la verifica delle firme

Chi intende utilizzare documenti sottoscritti con firma digitale generata utilizzando le chiavi certificate dal Certificatore ha l'onere di verificare la validità ed efficacia di dette chiavi e dei relativi certificati mediante scrupolosa consultazione del registro dei certificati del Certificatore e attendendosi alle modalità descritte nel capitolo 20.

Chiunque intende accedere al registro dei certificati per verificare una firma digitale è tenuto a (art. 38, comma 3, lett. d del DPCM 2004):

- **attenersi alle modalità indicate dal Certificatore per effettuare la verifica** (v. cap. 20)

- **verificare attentamente il contenuto del certificato relativo alla chiave pubblica** della coppia di chiavi utilizzata per la firma e, in particolare, la data di scadenza del certificato, l'esistenza ed il contenuto di eventuali limitazioni nell'uso della coppia di chiavi, poteri di rappresentanza ed abilitazioni professionali;
- **avvalersi di mezzi tecnici idonei a consentire la corretta, completa ed aggiornata consultazione di detto registro**. Il Certificatore non è in alcun caso responsabile di eventuali danni cagionati a chi intende verificare una firma digitale dall'utilizzo da parte dello stesso di mezzi a tal fine inadeguati ovvero dall'utilizzo improprio od erroneo dei mezzi tecnici impiegati;
- **verificare e utilizzare i certificati e le relative informazioni solo per le finalità in relazione alle quali i certificati sono rilasciati**.

È assolutamente vietato a chiunque di utilizzare i certificati emessi dal Certificatore per fini diversi da quelli previsti dal presente Manuale e dalla vigente normativa (art. 15, comma 2 e art. 29, comma 3 del DPCM 2004).

È assolutamente vietato a chiunque di accedere al registro dei certificati, alle liste dei certificati sospesi e revocati, per fini diversi dalla loro consultazione. In particolare, è vietata la loro modifica, estrazione, elaborazione, copia, diffusione ed in genere ogni trattamento ed utilizzazione diretta od indiretta, a qualsiasi fine, in difformità da quanto previsto nel presente Manuale Operativo, pena le sanzioni previste delle leggi vigenti.

10.6 Obblighi del terzo interessato

Il terzo interessato, sia esso persona fisica o giuridica, che acconsente alla emissione di uno o più certificati digitali intestati a persona che derivi i propri poteri da esso, a meno di normative o regolamenti che dispongano diversamente, ha l'obbligo di:

- **Prendere visione del presente Manuale Operativo e attenersi alle disposizioni contenute**.
- **Fornire al Certificatore le informazioni richieste** in fase di registrazione in modo esatto, completo e veritiero.
- **Chiedere la revoca dei certificati** ogniqualvolta vengano meno i requisiti in base ai quali il certificato era stato rilasciato al titolare, previa sua autorizzazione, per una delle seguenti circostanze; l'elencazione ha mero carattere esemplificativo:
  - ✓ Variazione o cessazione dei poteri di rappresentanza.
  - ✓ Variazione dei ruoli e delle qualifiche interne.
  - ✓ Cessazione del rapporto di dipendenza.
  - ✓ Ogni altro dato rilevante ai fini dell'uso del certificato.

Le richieste di revoca e/o di sospensione da parte del terzo interessato devono essere inoltrate corredate dalla relativa documentazione giustificativa, per iscritto o qualsiasi altro mezzo ritenuto idoneo dal Certificatore e, ove necessario, da questi messo a disposizione.

10.7 Definizione delle responsabilità e delle limitazioni agli indennizzi

Nel presente paragrafo sono individuate sia le limitazioni della responsabilità assunta dal Certificatore nell'ambito delle situazioni giuridiche relative allo svolgimento della propria attività, sia i correlati indennizzi, ferme restando le specifiche previsioni di cui ai precedenti paragrafi.

Il Certificatore non è in alcun modo responsabile per quanto di seguito indicato:

- danni di qualsiasi natura, diretti od indiretti, da chiunque patiti per eventi derivanti da **atti della Pubblica Autorità, caso fortuito, forza maggiore** ovvero da altra **causa non imputabile al Certificatore** (quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo del Certificatore, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi).
- danni di qualsiasi natura, diretti od indiretti, se non nei casi di **proprio dolo o colpa grave**.
- danni di qualsiasi natura, diretti od indiretti, da chiunque patiti nella misura in cui tali danni derivino dalla **violazione di obblighi** che, in virtù di quanto previsto dal presente Manuale Operativo ovvero

dalle vigenti disposizioni di legge, incombono al titolare, al richiedente la registrazione, al terzo interessato, a quanti accedono al registro dei certificati per la verifica della firma.

Il danneggiato decade dal diritto al risarcimento dei danni imputabili al Certificatore qualora non ne faccia motivata denuncia scritta al Certificatore entro il termine di 10 giorni dal verificarsi dell'evento dannoso ovvero da quando il danneggiato ne abbia avuto conoscenza.

Il Certificatore non assume alcun ulteriore obbligo, garanzia e responsabilità rispetto a quelli previsti dal presente Manuale Operativo o dalle vigenti disposizioni normative.

10.8 Manleva del titolare e dell'interessato

Il **titolare** manleva il Certificatore da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui il Certificatore sia chiamato a rispondere nei confronti di terzi, nei casi seguenti:

- fatto imputabile al titolare medesimo in relazione all'uso delle chiavi e/o del certificato.
- indicazione e/o dall'utilizzo dello pseudonimo da parte del titolare, qualora a questi sia consentito avvalersi di uno pseudonimo in luogo dei propri dati anagrafici (art. 27 bis, comma 1, lett. d del TUDA).

L'**interessato** manleva il Certificatore da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui il Certificatore sia chiamato a rispondere nei confronti di terzi per fatto imputabile all'interessato medesimo.

PARTE III

Modalità Operative del servizio di certificazione della firma digitale

11 Processo operativo dei Certificati Qualificati

I processi lavorativi del Certificatore possono suddividersi come segue:

1. **Creazione e consegna del dispositivo di firma**:
   1.1. richiesta di registrazione
   1.2. personalizzazione del dispositivo di firma
   1.3. consegna del dispositivo di firma al titolare;
2. **Gestione del certificato**
   2.1. revoca
   2.2. sospensione
3. i processi che riguardano la **conservazione dei documenti** previsti dalla normativa: il Giornale di Controllo e le Richieste di Registrazione.

11.1 Creazione e consegna del dispositivo di firma

Comprende le attività da effettuare dal momento in cui un titolare si presenta ad un Incaricato dell'Identificazione per sottoscrivere una richiesta di adesione, sino al momento in cui gli viene consegnato il dispositivo di firma.

11.1.1 Fase A1 - Richiesta di registrazione

Il processo ha gli scopi seguenti:

- ottemperare alla normativa vigente.
- raccogliere in un database indicizzato mediante il codice di registrazione del titolare, tutte le informazioni necessarie alla generazione del suo certificato.

Il processo è costituito dai seguenti sottoprocessi, effettuati secondo le procedure indicate più oltre:

- Adesione al servizio (sottoscrizione del modulo di adesione al servizio) da parte del Titolare
- Verifica dell'identità del titolare
- Compilazione della richiesta di registrazione
- Sottoscrizione della richiesta di registrazione

11.1.2 Fase A2 - Personalizzazione del dispositivo di firma

Il processo ha lo scopo di personalizzare il dispositivo sicuro di firma, che conserverà in modo protetto la chiave privata e consentirà di generare al suo interno firme digitali.

Il processo è costituito dai seguenti sottoprocessi:

- Generazione della coppia di chiavi di sottoscrizione
- Verifica dell'univocità della chiave pubblica
- Generazione delle richiesta di certificato nel formato PKCS#10
- Generazione del certificato e sua pubblicazione nel registro dei certificati
- Personalizzazione del dispositivo di firma.

11.1.3 Fase A3 - Consegna dei dispositivi di firma ai titolari

Scopo del processo è la consegna dei dispositivi di firma personalizzati ai titolari con modalità sicure tali da garantire che nessuna persona, ad eccezione del titolare, possa utilizzare la smartcard per firmare un documento informatico assumendo l'identità del titolare.

Il processo è costituito dai seguenti sottoprocessi:

- Spedizione dei dispositivi di firma agli Incaricati dell'identificazione
- Comunicazione dei codici riservati per l'utilizzo del dispositivo
- Consegna del dispositivo e dei codici al titolare.

11.2 Gestione del certificato

Il processo stabilisce le modalità di gestione della sospensione e della revoca dei certificati qualificati, coniugando l'esigenza di sicurezza in merito alla provenienza ed all'autenticità della richiesta, con la tempestività della sospensione o revoca del certificato nei casi di emergenza.

11.3 Conservazione dei documenti

Il processo stabilisce le modalità con cui il Certificatore assicura la conservazione dei documenti relativi al processo di creazione e consegna del dispositivo di firma, secondo quanto richiesto dalla normativa vigente. Tale processo non è oggetto di descrizione all'interno del presente Manuale Operativo

12 Modalità di Identificazione e Registrazione dei Titolari

Il processo si articola in due fasi principali:

- Nella prima fase, un incaricato del Certificatore procede all'**identificazione** della persona che intende divenire titolare di un certificato e alla compilazione della relativa richiesta di adesione al servizio.
- Nella seconda fase, il responsabile della Registrazione dei Titolari presso il Centro Servizi del Certificatore effettua l'**esame la documentazione prodotta** nella prima fase e, fatti i dovuti accertamenti, autorizza l'emissione del certificato per il richiedente.

12.1 Verifica dell'Identità del Sottoscrittore

I certificati possono essere emessi soltanto dopo l'identificazione del soggetto richiedente, che può essere effettuata dal Certificatore o da parte di propri incaricati, detti "Incaricati dell'identificazione e della consegna dei dispositivi di firma", i quali:

- **Sono afferenti alla struttura del cliente nel caso di soggetto appartenente alla pubblica amministrazione** che acquista i certificati dal Certificatore;
- **Sono afferenti alla strutture del cliente nel caso di associazioni professionali o aziende private** per i quali il Certificatore abbia verificato la sussistenza di requisiti di idoneità ed affidabilità per quanto concerne le attività di Identificazione e Registrazione esclusivamente dei **Titolari direttamente afferenti all'organizzazione del cliente stesso**.
- **Sono afferenti all'organizzazione del Certificatore**;

In ogni caso, l'autenticazione delle richieste di adesione e registrazione, nonché l'autorizzazione all'emissione dei certificati sono responsabilità del Certificatore, nella persona del responsabile della Registrazione dei Titolari.

Il Certificatore o un Incaricato effettuano l'identificazione e la registrazione secondo le modalità previste nel presente manuale operativo per le seguenti categorie di soggetti:

1. Richiedente il certificato in qualità di **persona fisica**.
2. Richiedente il certificato in qualità di **rappresentante e/o delegato di una persona fisica e/o giuridica**, previo consenso della stessa (cd. terzo interessato).
3. Richiedente il certificato in qualità di **appartenente ad una organizzazione e per il ruolo** che riveste all'interno della stessa.

12.1.1 Identificazione del richiedente quale persona fisica

Il richiedente in qualità di persona fisica, purché abbia compiuto il diciottesimo anno di età, compila e sottoscrive il Modulo di Richiesta di Adesione e lo sottopone all'Incaricato che provvede ad accertare la sua identità mediante l'esibizione in originale di uno dei documenti d'identificazione indicati dall'art. 35 del TUDA[2] in corso di validità.

[2] Alla data di emissione del presente Manuale Operativo sono considerati validi ai fini dell'identificazione, i seguenti documenti: carta di identità, passaporto, patente di guida, patente nautica, libretto di pensione, patentino di abilitazione alla conduzione di impianti termici, porto d'armi, tessere di riconoscimento purché munite di fotografia e di timbro o di altra segnatura equivalente e rilasciate da un'amministrazione dello Stato.

Il richiedente esibisce anche il Codice Fiscale in originale. I titolari residenti all'estero cui non risulti attribuito il codice fiscale, devono esibire un il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo quali il codice di sicurezza sociale, il codice identificativo generale, ecc. (art. 27 comma 2 del TUDA)

Al momento della registrazione, il richiedente specifica se, **per impieghi diversi**, ha necessità di possedere più certificati.

12.1.2 Identificazione del richiedente in qualità di rappresentate e/o delegato di persone fisiche e/o giuridiche

Ove il richiedente fosse interessato al rilascio di un certificato destinato a firmare in funzione di un ruolo, specificato nel certificato medesimo, inerente poteri di rappresentanza di **terzi** (**persone fisiche**), è tenuto a fornire, oltre alla documentazione di cui al punto precedente, anche la documentazione giustificativa dei poteri di rappresentanza, rilasciata con il consenso del terzo. Se i detti poteri di rappresentanza riguardano invece **persone giuridiche, altri titoli relativi all'attività professionale oppure cariche rivestite presso o per conto di organizzazioni terze**, il sottoscrittore è tenuto a fornire al Certificatore la documentazione che comprovi la sussistenza di poteri, cariche o titoli, nonché il consenso del terzo interessato.

Tale documentazione deve includere la nomina ufficiale all'incarico in questione o la dichiarazione ufficiale comprovante il titolo ricevuto.

Ai fini della corretta attuazione della normativa inerente la revoca del certificato e la sua sospensione, il Certificatore si riserva di procedere all'esatta **identificazione del terzo interessato**.

Eventuali denominazioni o marchi registrati possono essere inclusi nel certificato relativo a chiavi di sottoscrizione sulla base della documentazione comprovante la loro registrazione .

L'ammissibilità dell'**uso di pseudonimi** è valutata caso per caso dal Certificatore.

12.1.3 Identificazione del richiedente il certificato in qualità di appartenente ad una organizzazione

Nel caso di rilascio di certificati per ruoli o cariche rivestite per conto di organizzazioni terze (quali ad esempio aziende, associazioni, enti ecc.), il richiedente è tenuto a fornire, oltre alla documentazione di cui al paragrafo 12.1.1, anche la documentazione necessaria all'identificazione dell'organizzazione medesima, nonché una lettera ufficiale su carta intestata della Organizzazione di appartenenza nella quale siano contenuti i seguenti dati:

- Cognome e nome della persona per la quale si chiede la certificazione;
- Posizione all'interno della Organizzazione;
- Eventuale carica ricoperta all'interno dell'Organizzazione
- Eventuali limitazioni all'uso della coppia di chiavi;

ed inoltre i seguenti dati dell'Organizzazione:

- Ragione sociale;
- Indirizzo della sede legale;
- Numero di partita IVA;
- Numero di iscrizione al Registro delle Imprese;
- Estremi del rappresentante legale;
- La persona che, nel ruolo di "terzo interessato" ha la facoltà di richiedere la sospensione e/o la revoca dei certificati oltre al Titolare.

La lettera deve essere firmata dal Rappresentante Legale dell'Organizzazione o da altra persona munita di apposita procura autenticata da pubblico ufficiale e contenere, in allegato, il certificato di iscrizione al Registro delle Imprese.

12.2 Modalità di raccolta e verifica dei documenti identificativi forniti dal sottoscrittore

Il Certificatore raccoglie e conserva copia di ciascun documento originale di identificazione fornito dal sottoscrittore, firmata dall'Incaricato che ha eseguito l'identificazione con una modalità coerente con il supporto della copia.

Il Certificatore rilascia al sottoscrittore un elenco ufficiale dei documenti di identificazione raccolti, firmato dall'incaricato con una modalità coerente con il supporto che contiene l'elenco stesso.

La data di inizio validità del certificato è concordata all'atto della stipula del contratto di acquisto dei certificati e dei servizi ad essi connessi. Con l'accettazione della richiesta di registrazione dei singoli titolari dei certificati, il Certificatore si impegna a verificare e convalidare o rigettare tale richiesta in tempo utile all'emissione del certificato entro la data di inizio validità concordata.

Il rispetto di tali tempi è vincolato alla fornitura, da parte del singolo sottoscrittore di informazioni complete e accurate, e alla disponibilità a fornire tempestivamente eventuali integrazioni alla documentazione richiesta dal Certificatore medesimo.

Il rispetto dei tempi è altresì vincolato al pagamento del servizio di certificazione secondo le modalità pattuite.

12.3 Compilazione della Richiesta di Registrazione

12.3.1 Elenco delle Informazioni richieste al sottoscrittore

All'atto della registrazione, il sottoscrittore deve compilare il Modulo di Richiesta di Registrazione preparato dal Certificatore.

La tabella seguente elenca le informazioni contenute nel Modulo di Richiesta di Registrazione, che **devono essere fornite obbligatoriamente** (art. 27 bis, comma 1, lett. d del TUDA):

Campo
Nome
Cognome
Codice Fiscale
Data di nascita
Documento di Identità
Numero Documento

Nel caso di richiesta di **Certificati per ruoli o cariche rivestite per conto di organizzazioni terze**, il sottoscrittore è tenuto a compilare anche i campi necessari all'identificazione della organizzazione in oggetto, elencati nella tabella seguente:

Campo
Nome dell'organizzazione
Nome della divisione, unità, ufficio di competenza
Ragione Sociale (se applicabile)
Partita IVA (se applicabile)
Sede (Via/P.za)
Numero civico

C.A.P.
Comune
Provincia
Stato
Recapito Telefonico
N° iscrizione Camera di Commercio (se applicabile)
N° iscrizione al Tribunale (se applicabile)

La tabella seguente elenca **le informazioni** contenute nel Modulo di Richiesta di Registrazione, **obbligatorie** solo nel caso in cui il sottoscrittore richieda un certificato destinato a firmare in funzione di un ruolo o titolo relativi all'attività professionale o a cariche rivestite presso terzi:

Campo
Abilitazione Professionale /Ruolo/Poteri di rappresentanza
Prova dell'abilitazione, ruolo, incarico

Per quanto concerne l'indicazione dei ruoli, il Certificatore si attiene a quanto contenuto nelle "Linee guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei titolari dei certificati di firma elettronica" e alla relativa "Tabella dei ruoli e dei poteri" emesse da **Assocertificatori** (http://www.assocertificatori.it/doc/weblineegiuda080703.pdf).

All'atto della registrazione, l'Incaricato dell'Identificazione compila il Modulo di Richiesta di Registrazione utilizzando i dati forniti dal sottoscrittore durante la fase di identificazione.

La richiesta di registrazione deve essere firmata dal sottoscrittore alla presenza dell'Incaricato dell'identificazione. Unitamente alla richiesta sottoscritta, il Certificatore conserva anche copia sottoscritta e datata dal richiedente di tutti i documenti presentati nel corso della procedura di identificazione e registrazione.

La richiesta ed i dati di registrazione ivi contenuti sono conservati e trattati a cura del Certificatore e vengono utilizzati per la generazione del certificato relativo a chiavi di sottoscrizione, nonché per ogni comunicazione da parte del Certificatore al sottoscrittore, in conformità a quanto disposto dalla normativa vigente.

All'atto della compilazione del Modulo di Richiesta di Registrazione, il sottoscrittore riceve un codice univoco (**codice di registrazione**), che lo identificherà come titolare presso il Certificatore. I sistemi informatici del Certificatore garantiscono l'univocità di tale codice nell'ambito dei propri utenti. Qualora il medesimo soggetto sia titolare di più certificati, relativi a più ruoli per i quali egli può firmare, gli sono attribuiti codici identificativi distinti per ciascuno dei certificati.

12.3.2 Impegni assunti all'atto della firma della richiesta di registrazione

12.3.2.1 Da parte del sottoscrittore

Con la firma del Modulo di Richiesta di Registrazione, il sottoscrittore attesta:

- di avere **preso visione del Manuale Operativo** del Certificatore e aver **ricevuto informazioni accurate e complete** riguardo al servizio di certificazione;
- di conoscere i **principi generali** di funzionamento del servizio;
- di conoscere gli **obblighi** e le **responsabilità** che egli assume in merito alla protezione della segretezza della chiave privata e alla conservazione e uso dei dispositivi di firma, previsti dalla legge e riportati nel capitolo 10 del presente Manuale Operativo.

L'emissione del Certificato è vincolata al consenso del sottoscrittore al trattamento dei suoi dati, secondo quanto previsto dal DL 196/03, nei limiti e modi riportati nel capitolo 26 del presente Manuale Operativo e

illustrati nella informativa allegata al Modulo di Richiesta di Registrazione. Tale consenso è espresso mediante la firma di un apposito modulo.

La compilazione e firma del Modulo di Richiesta di Registrazione è considerata prova dell'assenso all'emissione del certificato, indipendentemente dal fatto che il sottoscrittore, successivamente, rifiuti di ritirare il certificato emesso.

12.3.2.2 Da parte dell'incaricato della identificazione

L'incaricato dell'identificazione controfirmando il Modulo di Richiesta di Registrazione attesta che:

- il sottoscrittore è la persona identificata nella richiesta;
- le informazioni incluse nella richiesta sono accurate, eccettuate eventuali informazioni non verificate comprese nella documentazione fornita dal sottoscrittore relativa a ruoli, titoli e incarichi da esso ricoperti. In tal caso le informazioni non verificate sono evidenziate sull'elenco lista dei documenti cartacei allegati alla richiesta.

Una volta terminata la fase di registrazione l' incaricato dell'identificazione non ha alcun ulteriore obbligo di verifica della validità delle informazioni contenute nella richiesta di registrazione ed eventualmente nel Certificato.

12.4 Approvazione della Richiesta di registrazione

In seguito alla raccolta del Modulo di Richiesta di Registrazione e dei documenti allegati, il Certificatore, fatte le verifiche ritenute necessarie, approva o rigetta la richiesta. Le verifiche sono condotte dal Responsabile della Registrazione dei Titolari, che fa parte dell'organizzazione del Certificatore e di norma opera presso il Centro Servizi del medesimo.

In qualunque caso, il Certificatore si riserva il diritto di:

- richiedere conferma delle informazioni personali fornite dal sottoscrittore confrontandole con dati raccolti presso terze parti o presso la Pubblica Autorità;
- verificare l'indirizzo postale, il numero telefonico, il nome e altre informazioni relative a organizzazioni terze, incluse informazioni specifiche relative a poteri, titoli o cariche ricoperte;
- richiedere alla terza parte, se presente, la verifica di particolari informazioni relative alla posizione del singolo sottoscrittore all'interno dell'organizzazione.

In caso di approvazione della richiesta, viene avviata la procedura di emissione del certificato, che sarà inserito nel dispositivo di firma contenente la chiave privata associata alla chiave pubblica cui il certificato medesimo si riferisce.

In caso di rigetto della richiesta, il Certificatore informa tempestivamente il sottoscrittore riportando il motivo del rigetto. Nel caso che il motivo del rigetto derivi da una verifica avvenuta tramite il coinvolgimento di terza parte interessata, il Certificatore fornisce al sottoscrittore le informazioni relative alle modalità di verifica seguite, in modo da favorire una rapida risoluzione di eventuali controversie.

Il sottoscrittore al quale sia stata rigettata una richiesta di registrazione ha il diritto di riformulare tale richiesta.

Il Certificatore si riserva il diritto di rifiutare l'emissione di un certificato declinando qualsiasi responsabilità per ogni eventuale pregiudizio diretto o indiretto che possa derivare da tale rifiuto.

13 Modalità di Generazione delle Chiavi

Questa sezione descrive le modalità seguite dal Certificatore per la generazione delle coppie di chiavi crittografiche.

Le coppie di chiavi generate appartengono ad una delle tre tipologie seguenti (art. 4, comma 4 del DPCM 2004):

- **Chiavi di certificazione**, generate dal Certificatore per il solo uso interno e adibite alla firma dei certificati relativi a chiavi di sottoscrizione e di marcatura temporale emessi dal Certificatore e delle relative liste di revoca e sospensione. Le chiavi di certificazione adibite alla firma dei certificati relativi a chiavi di sottoscrizione e quelle relative a chiavi di marcatura temporale sono formalmente identiche, pur essendo adibite solo e unicamente alla firma di una delle due tipologie di certificato.

- **Chiavi di marcatura temporale**, generate dal responsabile del Servizio di Marcatura Temporale interno del Certificatore, adibite all'apposizione di marche temporali.
- **Chiavi di Sottoscrizione**, generate dal Certificatore per conto dei sottoscrittori come previsto dal Modulo di Adesione.

La generazione delle coppie di chiavi e la verifica del corretto funzionamento delle coppie generate è attuata in conformità con le norme vigenti, ed in particolare con i seguenti articoli del DPCM 2004:

- Art. 3, Norme tecniche di riferimento;
- Art. 5, Generazione delle chiavi;
- Art. 6, Modalità di generazione delle chiavi;
- Art. 7, Conservazione delle chiavi;
- Art. 9, Dispositivi sicuri e procedure per la generazione della firma;
- Art. 13, generazione delle chiavi di certificazione;
- Art. 14, Generazione dei certificati qualificati;

nonché dall'art. 29-sexies del TUDA.

Le suddette chiavi sono generate dal Certificatore con una lunghezza di almeno 1.024 bit. I sistemi e le procedure utilizzate per le tipologie di chiavi garantiscono che:

- le coppie di chiavi sono generate singolarmente, ciascuna in unica copia (art. 5 del DPCM 2004);
- le chiavi private permangono segrete per l'intero loro ciclo di vita (art. 29-sexies, comma 1 del TUDA);
- in nessun caso è consentita la duplicazione di una chiave privata (art. 7, comma 1 del DPCM 2004);
- la chiave privata di ciascuna coppia è conservata in un dispositivo che ne garantisce la protezione e conservazione sicura (art. 29-sexies, comma 1 del TUDA);
- le coppie di chiavi rispondono ai requisiti imposti dagli algoritmi di generazione e di verifica RSA (Rivest-Shamir-Adleman algorithm) (art. 6, comma 4 e art. 9, comma 3 del DPCM 2004);
- la generazione di tutte le coppie possibili di chiavi è equiprobabile, allo stato attuale delle conoscenze scientifiche e tecnologiche (art. 5 del DPCM 2004);
- il soggetto che attiva la procedura di generazione è sempre identificato (art. 9, comma 7 del DPCM 2004).

13.1 Generazione delle Chiavi di Certificazione e Marcatura Temporale

Le modalità di generazione delle chiavi di certificazione e marcatura temporale sono analoghe, poiché, in entrambi i casi, le chiavi sono generate per uso interno del Certificatore o del suo Servizio di Marcatura Temporale. La generazione di entrambe le tipologie di chiavi è effettuata esclusivamente dal responsabile del relativo servizio (art. 6, comma 1 e art. 46, comma 4 del DPCM 2004).

13.1.1 Utilizzi specifici delle chiavi di certificazione

È prevista la generazione di due categorie di chiavi di certificazione (art. 6 comma 1 del DPCM 2004):

- chiavi dedicate alla firma di certificati di sottoscrizione e di autenticazione, nonché delle liste di revoca e sospensione, in conformità con la previsione di cui all'art. 4 comma 6 del DPCM 2004;
- chiavi dedicate alla firma di certificati di marcatura temporale.

Le due categorie di chiavi sono generate in maniera identica, ma utilizzate esclusivamente per le distinte attività a cui sono dedicate.

I certificati relativi a chiavi di certificazione sono inviati al CNIPA, che ne cura la pubblicazione nell'elenco pubblico dei Certificatori, successivamente inoltrato agli altri Certificatori presenti nell'Elenco Pubblico dei Certificatori.

13.1.2 Caratteristiche dei dispositivi di firma

Gli apparati in uso presso il Certificatore possiedono le caratteristiche seguenti:

- prevedono che la generazione delle coppie di chiavi avvenga esclusivamente all'interno del dispositivo preposto alla conservazione della chiave privata e all'apposizione delle firme digitali.

- sono dotati di motore interno di generazione di coppie di chiavi RSA e DSA. Tali dispositivi sono conformi ai requisiti di sicurezza imposti dalla normativa.
- sono a prova di manomissione e garantiscono la protezione e la custodia delle chiavi secondo i livelli di sicurezza previsti dalla normativa e secondo elevati standard tecnologici.

13.1.3 Sicurezza logica e fisica delle chiavi

L'accesso alle funzioni di firma dei dispositivi contenenti chiavi di certificazione è protetto dalla presenza di sistemi di attivazione a codice segreto, le cui procedure di gestione sono riservate e stabilite autonomamente dal Certificatore.

L'accesso agli applicativi di gestione del Centro Servizi è protetto da un sistema di sicurezza a livelli multipli, basato sull'utilizzo congiunto di:

- sistemi di autenticazione a livello di applicativo;
- dispositivi hardware personali di autenticazione basata su algoritmi crittografici;
- server di sicurezza dedicati esclusivamente alle procedure di autenticazione.

L'accesso ai locali del Centro Servizi è protetto da procedure di autorizzazione basate su liste di accesso multi livello. L'accesso ai locali ad alta sicurezza è protetto da:

- sistemi biometrici di autenticazione;
- serrature elettroniche autoalimentate a combinazione multipla;
- politiche di gestione degli accessi che definiscono con precisione l'identità dei singoli operatori e responsabili ammessi nei diversi locali. Nel locale in cui sono allocati i dispositivi contenenti i dati "sensibili" (data base, hsm, ecc.) è richiesta la presenza contemporanea di almeno due persone..

Tutti gli eventi relativi ad accessi, sia a livello logico che fisico, sono registrati nel giornale di controllo ed in registri cartacei soggetti a rigorose procedure di conservazione e controlli ispettivi periodici.

13.1.4 Custodia delle chiavi

Gli obblighi inerenti la custodia delle chiavi, previsti dalla normativa vigente, e descritti nel capitolo 10 del presente Manuale Operativo ricadono:

- sul responsabile della Generazione e Custodia delle Chiavi, per quanto concerne le chiavi di certificazione.
- sul responsabile del Servizio di Marcatura Temporale, per quanto concerne le chiavi di marcatura temporale.

13.2 Generazione di Chiavi di Sottoscrizione

La generazione delle chiavi di sottoscrizione avviene secondo modalità che garantiscono livelli di sicurezza analoghi a quelli previsti per la generazione di chiavi di certificazione e marcatura temporale. I dispositivi di firma sono custoditi all'interno di appositi locali protetti.

Le chiavi sono generate dal certificatore (art. 6, commi 2 e 3 del DPCM 2004) internamente al dispositivo sicuro di firma e sono attribuite ad un unico Titolare (art. 4, comma 1 del DPCM 2004).

- Le modalità di controllo degli accessi ad applicativi e locali utilizzati per la generazione e conservazione delle chiavi di sottoscrizione sono gestite secondo procedure uguali a quelle utilizzate per le chiavi di certificazione e marcatura temporale.

Nel caso specifico delle chiavi di sottoscrizione, gli obblighi inerenti la custodia delle chiavi, previsti dalla vigente normativa sono descritti nel capitolo 10 del presente Manuale Operativo e ricadono:

- sul responsabile della generazione e custodia delle chiavi, per quanto concerne la fase di generazione delle chiavi, di attribuzione dei dispositivi di firma contenenti le chiavi ai singoli sottoscrittori e di consegna;
- sui singoli sottoscrittori/titolari dal momento in cui essi entrano in possesso delle chiavi in poi.

L'utilizzo delle chiavi per l'apposizione di firme tramite procedure automatiche non solleva il titolare da obblighi e responsabilità inerenti la custodia delle chiavi.

13.2.1 Caratteristiche dei dispositivi sicuri di firma

I dispositivi di firma utilizzati sono smartcard o altri dispositivi analoghi in grado di conservare in modo protetto la chiave privata e di generare al proprio interno firme digitali, secondo la definizione indicata nella normativa vigente (art. 29 sexies del TUDA e art. 9 commi 1, 2 e 4 del DPCM 2004). La personalizzazione del dispositivo è annotata nel giornale di controllo (art. 9, comma 6 del DPCM 2004).

L'accesso alle funzioni di firma dei dispositivi sicuri è protetto dalla presenza di un codice segreto di attivazione, denominato Codice PIN, rivelato unicamente al Titolare. L'inserimento consecutivo di un numero predeterminato di PIN errati provoca il blocco del dispositivo di firma, che può essere poi sbloccato dal Titolare mediante l'apposito codice PUK di sblocco, comunicato insieme al PIN.

Restano pertanto valide tutte le garanzie di conformità alla normativa e ai requisiti di sicurezza elencate nel paragrafo 13.1 e riportate esplicitamente nel seguito:

- tutti i dispositivi coinvolti sono conformi ai requisiti di sicurezza imposti dalla normativa;
- le coppie di chiavi sono generate all'interno dei dispositivi; le chiavi private non abbandonano mai il dispositivo;
- i dispositivi utilizzati garantiscono la protezione e la custodia delle chiavi secondo i livelli di sicurezza previsti dalla normativa e secondo i più elevati standard tecnologici correnti. Idonei sistemi di sicurezza impediscono qualsiasi tentativo di lettura, duplicazione, estrazione della chiave privata.

14 Modalità di Emissione dei Certificati

Un certificato è un documento elettronico creato allo scopo di associare una chiave pubblica all'identità di un individuo. Tale documento, generato ed emesso dal Certificatore, è sottoscritto con firma digitale dal Certificatore medesimo e contiene informazioni sul titolare, inclusa la chiave pubblica a cui si riferisce tramite l'apposizione di una firma digitale.

A seguito dell'apposizione di una firma digitale a un'evidenza informatica, una copia del certificato è allegata in calce all'evidenza stessa. Tramite tale copia, l'utente a cui l'evidenza informatica è indirizzata è in grado di verificare l'identità dell'individuo che ha apposto la firma al documento.

Le modalità di emissione dei certificati sono regolamentate dai seguenti articoli del DPCM 2004:

- Art. 14, Generazione dei certificati qualificati;
- Art. 15, Informazioni contenute nei certificati;
- Art. 27, Requisiti di sicurezza dei sistemi operativi;
- Art. 28, Sistema di generazione dei certificati qualificati;

nonché dalle seguenti disposizioni del TUDA:

- Art. 27 bis, Certificati qualificati;

14.1 Tipologia e Struttura dei Certificati

I Certificati emessi dal Certificatore e oggetto del presente Manuale Operativo sono conformi alla normativa vigente e, in particolare, alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

La struttura dei certificati è conforme allo standard internazionale X.509 Versione 3.

Di seguito sono elencati i dati standard riportati nel certificato, secondo quanto previsto dalla normativa (art. 27 bis, commi 1, 2 e 3 del TUDA):

- ***Informazioni contenute in tutti i certificati:***
  - indicazione che si tratta di un certificato qualificato (v. il par. 1.1 per le modalità di identificazione dei certificati)
  - numero di serie del certificato;
  - ragione o denominazione sociale del Certificatore e Stato nel quale è stabilito;
  - codice identificativo del titolare presso il Certificatore;

- nome cognome e codice fiscale (o uno pseudonimo chiaramente indicato come tale) ovvero ragione o denominazione sociale del titolare (ove applicabile);
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- data di inizio e fine della validità delle chiavi;
- algoritmo di sottoscrizione del certificato;
- tipologia di utilizzo delle chiavi;
- firma elettronica avanzata del certificatore che ha rilasciato il certificato.

- ***Informazioni contenute nei certificati relativi a chiavi di sottoscrizione:***
  - eventuali poteri di rappresentanza;
  - eventuali abilitazioni professionali.
- ***Informazioni contenute nei certificati relativi a chiavi di certificazione***
  - esplicita menzione dell'uso delle chiavi per la certificazione.
- ***Informazioni contenute nei certificati relativi a chiavi di marcatura temporale***
  - esplicita menzione dell'uso delle chiavi per la marcatura temporale;
  - identificativo del sistema di marcatura temporale che utilizza le chiavi.

Per il **titolare residente all'estero cui non risulta attribuito il codice fiscale**, si indica il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza. Se questo non è disponibile, si indica un analogo codice identificativo (codice di sicurezza sociale o codice identificativo generale – art. 27 bis, comma 2 del TUDA).

Su domanda del titolare o del terzo interessato il certificato può contenere le seguenti informazioni, purché pertinenti allo scopo per il quale il certificato é richiesto (art. 27 bis, comma 3 del TUDA):

- le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
- limiti d'uso del certificato, ai sensi dell'articolo 28-bis, comma 3;
- limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

14.1.1 Utilizzo di pseudonimi

Qualora il richiedente, a norma dell'art. 9 del Codice Civile (Tutela dello pseudonimo), intenda utilizzare uno pseudonimo chiaramente identificato come tale e dimostri che lo pseudonimo per il quale richiede l'inserimento nel certificato qualificato è usato in modo che abbia acquistato l'importanza del proprio nome, il Certificatore lo riporta sul certificato elettronico qualificandolo come tale e conserva le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso (art. 27 bis, comma 1 lett. d e art. 29 ter, comma 1 del TUDA).

È invece **del tutto esclusa la possibilità che il titolare possa richiedere l'inserimento di un soprannome** (più propriamente "detto di famiglia") all'interno del certificato qualificato, poiché questo non può essere considerato un dato anagrafico e, ai fini dell'utilizzo del certificato qualificato, non costituisce strumento per evitare inconvenienti relativi ai casi di omonimia, essendo disponibili ulteriori dati per una corretta identificazione del titolare.

14.2 Generazione e Pubblicazione dei Certificati Qualificati relativi a Chiavi di Sottoscrizione

Dopo l'approvazione di una richiesta di registrazione, il Certificatore emette il certificato, con il che sancisce la definitiva convalida della richiesta di registrazione da parte del Certificatore.

Ogni certificato emesso è firmato da una chiave di certificazione del Certificatore.

Contestualmente all'emissione del certificato, il Certificatore provvede alla sua pubblicazione nel registro dei certificati da lui emessi.

Le modalità di gestione del registro dei certificati sono riportate nel capitolo 18 del presente Manuale Operativo.

Il sistema operativo del sistema informatico di generazione dei certificati è conforme ai requisiti previsti dalla normativa vigente.

La generazione di un certificato è registrata nel giornale di controllo del Certificatore. La traccia dell'avvenimento è conservata per almeno dieci anni dalla data di scadenza del certificato, secondo quanto previsto dalla normativa (art. 15, comma 5 del DPCM 2004).

Emettendo il certificato, il Certificatore garantisce al titolare che:

- il **certificato non contiene errori o inesattezze originati dal Certificatore** o giunti in qualsiasi modo a conoscenza del Certificatore;
- **il certificato è conforme a tutti i requisiti illustrati nel presente Manuale Operativo nonché a quanto richiesto dalla normativa vigente**;
- l'esecuzione di tutte le procedure finalizzate al rilascio del certificato da parte dell'organizzazione del Certificatore è stata eseguita a regola d'arte.

14.3 Consegna dei dispositivi di firma contenenti i certificati relativi a chiavi di sottoscrizione e delle informazioni per il loro utilizzo

14.3.1 Modalità di consegna dei dispositivi

Ogni certificato, emesso in seguito alla richiesta di registrazione da parte del relativo titolare, è inserito nel dispositivo sicuro di firma contenente la chiave privata relativa alla chiave pubblica riportata nel certificato medesimo.

I dispositivi di firma ed i codici segreti per l'utilizzo del servizio sono consegnati ai relativi titolari con modalità sicure, allo scopo di garantire che nessuna persona, ad eccezione del titolare, possa venirne contemporaneamente in possesso.

La consegna ai Titolari dei dispositivi sicuri di firma e dei codici segreti per l'utilizzo dei servizi è svolta dal Certificatore conformemente a quanto descritto nel paragrafo 10.3 del presente Manuale Operativo.

I codici segreti per l'utilizzo dei dispositivi di firma sono costituite da:

- codice segreto di **attivazione del dispositi**vo (codice **PIN**);
- codice segreto di **sblocco del dispositivo** (codice **PUK**);
- codice segreto di **revoca del certificato**
- password segreta e user ID del titolare per l'utilizzo del sistema di comunicazione sicuro con il Certificatore, tramite rete Internet, descritto nei capitoli 14.4 e 16 del presente Manuale Operativo.

Dal momento in cui li riceve, il Titolare è l'unico responsabile della protezione della segretezza di tali codici.

La consegna del dispositivo di firma può essere effettuata direttamente dal Certificatore nelle mani del Titolare, oppure per il tramite di un Incaricato dell'Identificazione. In questo caso, il Certificatore invia all'Incaricato dell'Identificazione il dispositivo mediante un intermediario di trasporto di sua fiducia. L'Incaricato procede alla convocazione del Titolare, si accerta della sua identità e verifica che sia la stessa persona che ha sottoscritto la richiesta di registrazione al servizio. Alla consegna del dispositivo di firma, gli fa sottoscrivere una dichiarazione mediante la quale il Titolare attesta di aver ricevuto il dispositivo, la sottoscrive a sua volta e ne produce una copia da consegnare al Titolare. Provvede quindi a inviare la dichiarazione in originale al Certificatore.

14.3.2 Consegna dei codici segreti

La consegna dei codici segreti può essere effettuata direttamente dal Certificatore nelle mani del Titolare, oppure per il tramite di un Incaricato dell'Identificazione. In questo caso, il Certificatore invia ad un Incaricato dell'identificazione diverso da quello delegato alla consegna del dispositivo di firma i codici segreti per l'utilizzo del servizio, tramite un intermediario di trasporto di sua fiducia. Questo 'Incaricato procede alla convocazione del Titolare, si accerta della sua identità e verifica che sia la stessa persona che ha sottoscritto la richiesta di registrazione al servizio. Al momento della consegna dei codici segreti, fa sottoscrivere una dichiarazione mediante la quale il Titolare attesta di aver ricevuto i codici e che il loro contenitore non presentava segni evidenti di effrazione, la sottoscrive a sua volta e ne produce una copia da consegnare al Titolare. Provvede quindi a inviare la dichiarazione in originale al Certificatore.

14.4 Generazione e Pubblicazione dei Certificati relativi a chiavi di Certificazione e Marcatura Temporale

Le modalità di pianificazione e autorizzazione all'emissione e pubblicazione dei certificati relativi a chiavi di certificazione e di marcatura temporale sono regolate da norme interne del Certificatore.

In ogni caso, la validità di detti certificati non supera il periodo di tempo previsto dalla normativa vigente.

I certificati relativo a chiavi di certificazione e di marcatura temporale sono firmati dalla chiave privata della coppia a cui si riferiscono e sono registrati presso il CNIPA.

I certificati relativi a chiavi di marcatura temporale sono firmati da una chiave di certificazione diversa da quelle utilizzate per la firma di certificati relativi a chiavi di sottoscrizione, in conformità alla normativa vigente.

Le modalità di pubblicazione dei certificati relativi a chiavi di certificazione e marcatura temporale e le caratteristiche tecniche dei sistemi di generazione utilizzati per l'emissione di tali certificati sono conformi a quanto previsto dalla normativa vigente per i certificati relativi a chiavi di sottoscrizione e riportato nel paragrafo 13.2 del presente Manuale Operativo.

15 Modalità di Revoca dei Certificati

Questa sezione descrive il processo di revoca dei certificati, specificando le circostanze in cui un certificato può e deve essere revocato e le modalità in cui la revoca deve essere richiesta, effettuata e notificata al titolare del certificato. La sezione include le informazioni di pubblica utilità sulle procedure di revoca dei certificati relativi a chiavi di certificazione e di marcatura temporale.

La revoca di certificati relativi a chiavi di sottoscrizione e di certificazione, o marcatura temporale è attuata in conformità con le norme vigenti. In particolare, si fa riferimento alle disposizioni seguenti:

- art. 22 del TUDA, Definizioni;
- art. 23 del TUDA, Firma digitale;
- art. 29-septies del TUDA, Revoca e sospensione dei certificati qualificati;
- art. 7, comma 3, lett. c del DPCM 2004, Conservazione delle chiavi;
- art. 15 del DPCM 2004, Informazioni contenute nei certificati qualificati;
- art. 16 del DPCM 2004, Revoca e sospensione del certificato qualificato;
- art. 17 del DPCM 2004, Revoca dei certificati qualificati relativi a chiavi di sottoscrizione;
- art. 18 del DPCM 2004, Revoca su iniziativa del certificatore
- art. 19 del DPCM 2004, Revoca su richiesta del titolare
- art. 20 del DPCM 2004, Revoca su richiesta del terzo interessato;
- art. 35 del DPCM 2004, Formato dei certificati qualificati.

15.1 Motivazioni di Revoca

Ai sensi della normativa vigente i certificati qualificati devono essere revocati quando ricorrono una o più delle seguenti circostanze:

- Cessazione dell'attività del Certificatore (art. 29 septies comma 1, lett. a del TUDA);
- Richiesta da parte del Titolare (art. 29 septies comma 1, lett. c del TUDA);
- Richiesta da parte del "terzo interessato" dal quale derivano i poteri del Titolare (art. 29 septies comma 1, lett. c del TUDA);
- Perdita di possesso della chiave;
- Provvedimento dell'Autorità (art. 29 septies comma 1, lett. b del TUDA);
- Acquisizione della conoscenza di cause limitative della capacità del Titolare (art. 29 septies comma 1, lett. d del TUDA);
- Sospetti abusi e/o falsificazioni (art. 29 septies comma 1, lett. d del TUDA).

Il Certificatore può procedere alla revoca del certificato nei seguenti casi:

- **Possibile compromissione della chiave privata** (art. 18 del DPCM 2004).
- Qualora la richiesta di revoca provenga da **terzi interessati secondo la normativa vigente**, quali, ad esempio:
  - un'organizzazione terza, dalla quale derivano in capo al Titolare i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite presso o per conto dell'organizzazione terza medesima.
  - l'organizzazione terza che ha stipulato il contratto di acquisto del certificato destinandolo ad una persona a lei, in qualunque maniera, afferente.
  - La persona fisica o giuridica rappresentata legalmente dal Titolare in virtù di una procura o di una delega.

Oltre alle circostanze sopra riportate, sono motivo di revoca del certificato:

- la modifica o la scadenza del rapporto che intercorre tra il titolare e l'organizzazione per conto di cui il certificato viene utilizzato;
- il decadere del titolo, della carica o del ruolo inerente i poteri di rappresentanza o la qualifica professionale in nome di cui il certificato viene utilizzato.
- Il ritiro della procura o della delega da parte del rappresentato

Inoltre, la **revoca** può avvenire **su iniziativa del Certificatore** quando si verifichino una o più delle circostanze seguenti:

- riscontro che il certificato non è stato rilasciato secondo le modalità previste dalla normativa vigente;
- riscontro che uno dei prerequisiti per l'accettazione della registrazione del titolare è venuto meno;
- sopravvenuta modifica di dati personali del titolare o di altri elementi riportati sul certificato;
- riscontro che il titolare del certificato ha infranto uno degli obblighi assunti al momento della richiesta di registrazione, previsti dalla normativa e riportati nel presente Manuale Operativo;
- compromissione della chiave di certificazione che ha firmato il certificato in questione;
- eventuale richiesta motivata e documentata dell'autorità giudiziaria.

Le cause di revoca elencate nel presente Manuale Operativo non sono da considerare tassative e non esauriscono le motivazioni per cui il titolare o il terzo interessato possono richiedere la revoca di un certificato relativo a chiavi di sottoscrizione.

Ai sensi della normativa il Certificatore procede alla **sospensione** del certificato (invece della revoca) nel caso in cui non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta di revoca (art. 19, comma 4 del DPCM 2004).

I certificati relativi a chiavi di marcatura temporale sono assoggettati alla medesima regolamentazione dei certificati relativi a chiavi di sottoscrizione. In tal caso, il titolare del certificato è il responsabile del servizio di marcatura temporale che ne fa uso.

15.2 Modalità generali di revoca ed effetti della revoca di un certificato

La revoca di un certificato determina la immediata e definitiva cessazione della sua validità, indipendentemente dalla data di scadenza del certificato medesimo. La revoca non inficia la validità del certificato nel lasso di tempo precedente il momento della revoca stessa art. 29 septies, comma 3 del TUDA).

La revoca viene effettuata mediante l'inserimento del certificato nella lista dei certificati revocati. La pubblicazione di tale lista determina il momento a partire dal quale il certificato si considera revocato (art. 28, comma 3 del TUDA). Le modalità di accesso a tale lista per la verifica della validità dei certificati sono descritte nel par. 18.5 e nel capitolo 20 del presente Manuale Operativo.

Qualora la revoca avvenga a causa della possibile compromissione della segretezza della chiave privata, il Certificatore garantisce l'immediata pubblicazione dell'aggiornamento della lista dei certificati revocati riportante la revoca in questione.

15.3 Revoca di Certificati relativi a Chiavi di Sottoscrizione

15.3.1 Ricezione e verifica di una richiesta di revoca

Il titolare o il terzo interessato che intenda ottenere la revoca di un certificato relativo a chiavi di sottoscrizione deve inoltrare regolare richiesta di revoca secondo le modalità descritte nel presente paragrafo.

Secondo quanto stabilito dalla normativa vigente, per ciascun certificato emesso il Certificatore fornisce al titolare un **codice segreto di revoca**, da utilizzare in caso di emergenza per l'autenticazione della eventuale richiesta di revoca del certificato. Tale codice è consegnato al Titolare in busta chiusa e sigillata, unitamente al codice di attivazione del dispositivo di firma (v. par. 14.3.2).

15.3.1.1 Revoca su richiesta del titolare

Le richieste di revoca provenienti direttamente dal titolare di un certificato sono accettate qualora siano redatte ed inoltrate **per iscritto** ed inoltre:

1) Contengano esplicita dichiarazione della volontà di revocare il certificato.
2) Contengano la motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca.
3) Contengano il *codice di registrazione* fornito al titolare al momento della richiesta di registrazione relativa al certificato da revocare.
4) Contengano almeno i seguenti dati anagrafici del richiedente:
   - nome e cognome;
   - data e luogo di nascita;
   - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
   - codice fiscale.

Qualora le richieste di revoca siano sottoposte al Certificatore secondo una delle seguenti procedure:

a) **tramite il canale di comunicazione sicuro con il Certificatore**, predisposto dal Certificatore medesimo all'atto dell'accettazione della registrazione del titolare. Tale canale, le cui specifiche tecniche sono riportate sul Modulo di Richiesta di Registrazione, è costituito da una connessione Internet con un'applicazione dedicata sul Server di Front End, gestito presso il Centro Servizi del Certificatore e operante secondo un protocollo https. La connessione del singolo titolare è soggetta ad autenticazione tramite un nome utente (userId) ed un codice segreto (password) comunicati al titolare congiuntamente al codice di abilitazione del dispositivo di firma (codice PIN);

b) **per telefono**, chiamando il numero verde del Centro Servizi del Certificatore, riportato nel sito: **http://www.firmasicura.it**, fornendo le informazioni elencate in precedenza nei punti da 1 a 4 e, in aggiunta, dichiarando esplicitamente il **codice segreto di revoca**.

   In tal caso, il Certificatore provvede a sospendere cautelativamente il Certificato mentre il titolare si impegna a confermare per iscritto la richiesta di revoca, inviandola tramite fax, al numero del Centro Servizi del Certificatore, riportato nel sito: **http://www.firmasicura.it**. **Qualora tale richiesta non venga confermata entro il lasso di tempo specificato nella tabella di cui sopra, il certificato rimarrà sospeso sino alla sua naturale scadenza.**

   Il fax deve contenere, le informazioni elencate in precedenza nei punti da 1 a 4 e, in aggiunta:

   - fotocopia del medesimo documento di riconoscimento fornito al momento della richiesta di registrazione, ovvero del nuovo documento in caso di rinnovo;
   - nel caso di richiesta di revoca motivata da smarrimento o furto del dispositivo di firma, la fotocopia della denuncia dell'avvenuto smarrimento o furto.

   Il Certificatore si riserva il diritto di non procedere alla revoca definitiva del certificato, bensì alla sua sospensione immediata sino al ricevimento della conferma della richiesta di revoca..

In qualunque caso, qualora il titolare intenda inoltrare una **richiesta di revoca immediata**, tale volontà deve essere riportata esplicitamente**.**

Sono comunque considerate richieste di revoca immediata quelle che adducono esplicitamente una delle motivazioni seguenti:

- possibile compromissione della segretezza della chiave privata;

- furto del dispositivo di firma;
- smarrimento del dispositivo di firma.

15.3.1.2 Revoca su richiesta del terzo interessato

Le richieste di revoca provenienti dal terzo interessato sono accettate qualora siano redatte ed inoltrate **per iscritto** ed inoltre:

1. contengano esplicita dichiarazione della volontà di revocare il certificato;
2. contengano la motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca;
3. contengano almeno i seguenti dati anagrafici del richiedente:
   - nome e cognome;
   - data e luogo di nascita;
   - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
4. contengano la documentazione giustificativa della revoca. Ad esempio: copia dei documenti ufficiali attestanti la modifica o terminazione del rapporto intercorrente tra titolare e terzo interessato per conto di cui il certificato viene utilizzato, o il decadere del titolo, della carica o del ruolo in nome del quale il certificato viene utilizzato, revoca della procura o della delega.

15.3.2 Attuazione della Revoca del Certificato

Il Certificatore si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della revoca riportati sulla relativa richiesta. Nei casi di compromissione della chiave privata, furto o smarrimento del dispositivo, il Certificatore si impegna ad eseguire la **revoca tempestivamente** all'atto della ricezione della richiesta.

La revoca del certificato è sancita dal suo inserimento in una Lista dei Certificati Revocati firmata da una chiave di certificazione e pubblicata.

Le liste di revoca sono conformi alla normativa vigente, ed in particolare alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Le Liste dei Certificati Revocati sono **pubblicate periodicamente**, secondo quanto riportato nel paragrafo 18.4.

Nel caso in cui la revoca debba essere immediata, la pubblicazione di una Lista dei Certificati Revocati può essere effettuata in maniera non programmata.

In ogni caso, l'inserimento di un certificato in una lista di revoca è registrato in un apposito archivio informatico del Certificatore. La traccia dell'avvenimento è conservata per almeno dieci anni dalla data di scadenza del certificato, secondo quanto previsto dalla normativa.

15.3.3 Notifica al Titolare

L'avvenuta revoca di un certificato relativo a chiavi di sottoscrizione viene notificata al titolare tramite telegramma, servizio Postel, altro canale postale o qualsiasi altro mezzo considerato idoneo dal Certificatore (art. 18, comma 1 DPCM 2004).

Analogamente viene notificato qualunque fatto noto al Certificatore che possa compromettere la validità o affidabilità del certificato.

15.3.3.1 Notifica anticipata

Secondo quanto previsto dalla normativa vigente, l'intenzione di revocare un certificato è notificata anticipatamente al titolare, salvo casi di motivata urgenza, ogni qual volta la revoca avvenga per iniziativa del Certificatore o del terzo interessato.

In ciascun caso, la notifica contiene:

- i dati identificativi univoci del titolare e del certificato in questione;
- i motivi della revoca;
- dati identificativi del richiedente la revoca;
- la data e l'ora a partire dalla quale il certificato non è più valido.

La revoca di un certificato viene comunicata a utenti terzi tramite la pubblicazione delle liste di revoca. La verifica della validità di un certificato è responsabilità di chiunque intenda fare affidamento sul medesimo. In particolare, è responsabilità dell'utente terzo il controllo dell'eventuale presenza del certificato su una lista di

revoca firmata dal Certificatore che l'ha emessa. Tale controllo deve includere la verifica che la lista in esame non sia scaduta a causa della pubblicazione, in data od ora successiva, di una lista più aggiornata.

Il Certificatore declina ogni responsabilità per fatti derivanti dall'eventuale accettazione da parte di utenti terzi di una firma digitale, senza l'adeguato controllo dello stato del certificato relativo.

15.4 Revoca di Certificati relativi a chiavi di Certificazione

La revoca dei certificati relativa a chiavi di certificazione si attua nei casi seguenti (art. 26 del DPCM 2004):

- compromissione della chiave privata (diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata);
- guasto del dispositivo di firma;
- cessazione dell'attività del Certificatore.

Nei predetti casi, il Certificatore provvede alla revoca del certificato relativo alle chiavi di certificazione e di tutti i certificati sottoscritti con la chiave privata appartenente alla coppia revocata.

L'operazione è notificata al CNIPA e a tutti i Titolari di certificati sottoscritti con la chiave privata appartenente alla coppia revocata, entro 24 ore dalla sua attuazione

16 Modalità di Sospensione dei Certificati

Questa sezione descrive il processo di sospensione dei certificati, specificando le circostanze in cui un certificato può o deve essere sospeso e le modalità in cui la sospensione deve essere richiesta, effettuata e notificata al titolare del certificato.

Le procedure di sospensione non si applicano ai certificati relativi a chiavi di certificazione e di marcatura temporale.

La sospensione di certificati qualificati è attuata in conformità con le norme vigenti. In particolare, si fa riferimento alle disposizioni seguenti:

- art. 22 del TUDA, Definizioni;
- art. 23 del TUDA, Firma digitale;
- art. 29-septies del TUDA, Revoca e sospensione dei certificati qualificati;
- art. 16 del DPCM 2004, Revoca e sospensione del certificato qualificato;
- art. 21 del DPCM 2004, Sospensione dei certificati qualificati,
- art. 22 del DPCM 2004, Sospensione su iniziativa del certificatore,
- art. 23 del DPCM 2004, Sospensione su iniziativa del titolare;
- art. 24 del DPCM 2004, Sospensione su richiesta del terzo interessato;
- art. 35 del DPCM 2004, Formato dei certificati qualificati
- art. 37 del DPCM 2004, Codice di emergenza

16.1 Motivazioni e Modalità di Sospensione

Il Certificatore utilizza in via cautelativa lo strumento della sospensione qualora una richiesta di revoca venga effettuata tramite le modalità di comunicazione telefonica , ovvero tramite il canale di comunicazione sicuro con il Certificatore riportate al paragrafo 15.3.1.1. In tal caso, il certificato viene sospeso temporaneamente. La revoca definitiva viene effettuata solo dopo la ricezione della conferma da parte del titolare.

Al di fuori del caso della sospensione telefonica in via cautelativa, preventiva alla conferma per iscritto della revoca, la sospensione del certificato può essere effettuata anche nei casi e dai soggetti seguenti:

- su **richiesta del Titolare** (art. 23 del DPCM 2004);
- su **richiesta dell'Incaricato** dell'Identificazione e della consegna dei dispositivi di firma;
- su **richiesta del terzo interessato** (art. 24 del DPCM 2004);
- su **iniziativa del Certificatore**.

La ***sospensione da parte del Titolare e dell'Incaricato*** può essere richiesta con le modalità seguenti:

- per **iscritto**, tramite fax inviato al Centro Servizi del Certificatore (riportato nel sito: http://www.firmasicura.it);
- utilizzando il **servizio telefonico** o il **canale web sicuro** messi a disposizione dal Certificatore.

Il Certificatore effettua la sospensione non appena riceve la richiesta. La sospensione ha effetto dalla pubblicazione della relativa CSL (Certificate Suspention List).

Nei casi di sospensione telefonica o via web, la richiesta deve essere confermata per iscritto tramite fax inviato al Centro Servizi del Certificatore (riportato nel sito: http://www.firmasicura.it).

Nella richiesta di sospensione per iscritto o nella conferma scritta della sospensione richiesta via telefono o via web devono essere chiaramente indicati:

- esplicita dichiarazione della volontà di sospendere il certificato (se la richiesta proviene dal Titolare);
- la motivazione della richiesta di sospensione ed il periodo di sospensione richiesto;
- il *codice di registrazione* del titolare;
- i seguenti dati anagrafici del **Titolare o dell'Incaricato se è lui a chiedere la sospensione**:
  - nome e cognome;
  - data e luogo di nascita;
  - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
  - codice fiscale;
- fotocopia di un documento di riconoscimento del **richiedente la sospensione** (preferibilmente lo stesso fornito al momento dell'identificazione);
- il momento a partire dal quale il certificato deve essere sospeso;
- il momento a partire dal quale il certificato deve essere riattivato.

La ***sospensione da parte del Terzo Interessato*** può essere richiesta esclusivamente per **iscritto**, tramite fax inviato al Centro Servizi del Certificatore (riportato nel sito: http://www.firmasicura.it), che deve contenere:

- esplicita dichiarazione della volontà di sospendere il certificato;
- la motivazione della richiesta di sospensione e il periodo di sospensione richiesto;
- i seguenti dati anagrafici del richiedente:
  - nome e cognome;
  - data e luogo di nascita;
  - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza).
- il momento a partire dal quale il certificato deve essere sospeso;
- il momento a partire dal quale il certificato deve essere riattivato.

In caso di omessa indicazione del momento della riattivazione, il certificato si intende sospeso sino alla sua naturale scadenza e potrà essere riattivato solo attraverso specifica richiesta scritta inoltrata al Certificatore con le modalità sopra riportate.

16.2 Sospensione di Certificati

La sospensione di un certificato determina l'immediata cessazione della sua validità, indipendentemente dalla data di scadenza del certificato medesimo, sino al momento della sua riattivazione. La sospensione non inficia la validità del certificato nel lasso di tempo precedente il momento della sospensione stessa.

La sospensione viene effettuata mediante l'inserimento del certificato nella lista dei certificati sospesi (CSL). La pubblicazione di tale lista determina il momento a partire dal quale il certificato si considera sospeso (art. 29 septies, comma 3 del TUDA).

Qualora la sospensione avvenga a causa della possibile compromissione della segretezza della chiave privata, il Certificatore garantisce l'immediata pubblicazione dell'aggiornamento della lista dei certificati sospesi riportante la sospensione in questione.

Le liste di sospensione sono conformi alla normativa vigente e, in particolare, alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Le Liste dei Certificati Sospesi sono pubblicate periodicamente, secondo tempistiche riportate nel presente Manuale Operativo, nel par. 18.4.

Nel caso in cui la sospensione debba essere immediata, la pubblicazione della nuova Lista dei Certificati Sospesi può essere effettuata in maniera non programmata.

L'inserimento di un certificato in una lista di sospensione è registrato in un apposito archivio informatico del Certificatore. La traccia dell'avvenimento è conservata per almeno dieci anni dalla data di scadenza del certificato, secondo quanto previsto dalla normativa.

16.2.1 Gestione dei certificati sospesi e delle relative chiavi di sottoscrizione

I certificati sospesi permangono nella relativa Lista dei Certificati Sospesi per l'intero periodo di sospensione.

Le chiavi private corrispondenti a chiavi pubbliche contenute in certificati sospesi e i dispositivi che le contengono, devono essere conservate con la massima diligenza da parte dei titolari anche durante il periodo di sospensione. Analogamente, le informazioni riservate di abilitazione all'uso della chiave privata devono essere salvaguardate e conservate in luogo diverso dal dispositivo che contiene la chiave, come previsto dalla normativa vigente.

16.2.2 Notifica al Titolare

L'avvenuta sospensione di un certificato relativo a chiavi di sottoscrizione viene notificata al titolare tramite telegramma, servizio Postel, altro canale postale o qualsiasi altro mezzo considerato idoneo dal Certificatore (art. 22, comma 1 del DPCM 2004).

Analogamente viene notificato qualunque fatto noto al Certificatore che possa compromettere la validità o affidabilità del certificato.

16.2.2.1 Notifica anticipata

Secondo quanto previsto dalla normativa vigente, l'intenzione di sospendere un certificato è notificata anticipatamente al titolare, salvo casi di motivata urgenza, ogni qual volta la sospensione avvenga per iniziativa del Certificatore o del terzo interessato (art. 22, comma 2 del DPCM 2004).

In ciascun caso, la notifica contiene:

- i dati identificativi univoci del titolare e del certificato in questione;
- i motivi della sospensione;
- dati identificativi del richiedente la sospensione;
- la data e l'ora a partire dalla quale il certificato non è più valido.

La sospensione di un certificato viene comunicata a utenti terzi tramite la pubblicazione delle liste di sospensione. La verifica della validità di un certificato è responsabilità di chiunque intenda fare affidamento sul medesimo. In particolare, è responsabilità dell'utente terzo il controllo dell'eventuale presenza del certificato su una lista di sospensione firmata dal Certificatore che l'ha emessa. Tale controllo deve includere la verifica che la lista in esame non sia scaduta a causa della pubblicazione, in data od ora successiva, di una lista più aggiornata.

Il Certificatore declina ogni responsabilità per fatti derivanti dall'eventuale accettazione da parte di utenti terzi di una firma digitale, senza l'adeguato controllo dello stato del certificato relativo.

16.3 Riattivazione di Certificati relativi a chiavi di Sottoscrizione sospesi

Il titolare e il terzo interessato possono richiedere la riattivazione anticipata di un certificato sospeso.

16.3.1 Richiesta di Riattivazione Anticipata

Il titolare, l'Incaricato dell'Identificazione o il terzo interessato che intendano ottenere la riattivazione anticipata di un certificato sospeso devono inoltrare regolare richiesta secondo le modalità di seguito indicate:

- le richieste di **riattivazione anticipata da parte del titolare** di un certificato o dall'Incaricato dell'Identificazione sono accettate qualora siano inviate tramite fax al numero del Centro Servizi del Certificatore, riportato nel sito http://www.firmasicura.it e contengano:
  - esplicita dichiarazione della volontà di riattivare anticipatamente il certificato;
  - la motivazione della riattivazione anticipata e la decorrenza richiesta;
  - il *codice di registrazione* del titolare;
  - i seguenti dati anagrafici del **richiedente**:
    - nome e cognome;
    - data e luogo di nascita;
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
    - codice fiscale.
  - fotocopia di un documento di riconoscimento, preferibilmente lo stesso fornito al momento dell'identificazione.
- le richieste di **riattivazione anticipata da parte del terzo interessato** sono accettate qualora pervengano al Certificatore tramite fax al numero del Centro Servizi del Certificatore, riportato nel sito http://www.firmasicura.it e contengano:
  - esplicita dichiarazione della volontà di riattivare anticipatamente il certificato;
  - la motivazione della richiesta di riattivazione anticipata e la decorrenza richiesta;
  - i seguenti dati anagrafici del richiedente:
    - nome e cognome;
    - data e luogo di nascita;
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza).

16.3.2 Riattivazione del Certificato

Il Certificatore si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della riattivazione anticipata riportati sulla richiesta di riattivazione.

La riattivazione del certificato è sancita dalla sua eliminazione dalla Lista dei Certificati Sospesi, firmata da una chiave di certificazione e pubblicata.

Le Liste dei Certificati Sospesi sono pubblicate periodicamente, secondo tempistiche riportate nel capitolo 18 del presente Manuale Operativo.

L'eliminazione di un certificato da una lista di sospensione è registrata in un apposito archivio informatico del Certificatore. La traccia dell'avvenimento è conservata almeno per dieci anni dalla data di scadenza del certificato, secondo quanto previsto dalla normativa.

16.3.3 Notifica al Titolare

La riattivazione di un certificato viene notificata al titolare tramite telegramma, servizio Postel, altro canale postale o qualsiasi altro mezzo che il Certificatore ritenga adeguato.

16.3.4 Notifica anticipata

Secondo quanto previsto dalla normativa vigente, l'intenzione di riattivare un certificato è notificata anticipatamente al titolare, salvo casi di motivata urgenza, ogni qual volta la richiesta provenga da un terzo interessato.

In ciascun caso, la notifica contiene:

- i dati identificativi univoci del titolare e del certificato in questione;
- i motivi della riattivazione;
- la data e l'ora a partire dalla quale il certificato riassume la sua validità.

17 Modalità di Sostituzione delle Chiavi

Questa sezione descrive il processo di sostituzione delle chiavi scadute con nuove coppie di chiavi e l'emissione del relativo certificato. Tale processo non può essere considerato come un'operazione di rinnovo

del certificato poiché, in base a quanto previsto dalla normativa vigente, non è ammessa la certificazione di chiavi che siano già state certificate in precedenza.

La sostituzione delle chiavi è attuata in conformità con le norme vigenti.

17.1 Sostituzione delle chiavi di sottoscrizione e di marcatura temporale

La procedura di richiesta di rinnovo della registrazione si svolge in maniera identica a quella di richiesta di prima registrazione, descritta nel capitolo 12 del presente Manuale Operativo. Il Certificatore attribuisce al titolare un nuovo codice identificativo univoco collegato al dispositivo di firma contenente la nuova coppia di chiavi e al relativo certificato di nuova emissione.

Nel caso in cui i dati del Titolare contenuti nel modulo di richiesta di registrazione ed utilizzati per l'emissione del certificato e per le comunicazioni con il Titolare non abbiano subito modifiche rispetto alla prima registrazione, non è necessario né effettuare una nuova registrazione né produrre una nuova documentazione di accompagnamento.

L'emissione del nuovo certificato avviene, di norma, utilizzando **un nuovo dispositivo di firma** Nel caso di **chiavi di marcatura temporale** il titolare del certificato è il responsabile del servizio di marcatura temporale per cui il certificato viene emesso.

17.2 Sostituzione delle chiavi di certificazione

La sostituzione di chiavi di certificazione è attuata in conformità con quanto regolamentato dalla normativa vigente (art. 25 del DPCM 2004).

La procedura di sostituzione di una coppia di chiavi di certificazione in scadenza è avviata almeno 90 giorni prima della scadenza del certificato ad essa relativa.

La procedura comporta la generazione di una nuova coppia di chiavi di certificazione e del certificato ad essa relativo, nonché di una coppia di certificati che attestino la sostituzione del certificato in scadenza, e la registrazione dei tre certificati presso il CNIPA.

17.2.1 Generazione della nuova coppia di chiavi

La nuova coppia di chiavi, in sostituzione della coppia in scadenza, è generata con le modalità ordinarie descritte nel paragrafo 13.1 del presente Manuale Operativo.

17.2.2 Generazione dei Certificati

Il certificato relativo alla nuova coppia di chiavi di certificazione viene emesso secondo le modalità ordinarie descritte nel capitolo 14 del presente Manuale Operativo.

In aggiunta a tale certificato, viene emesso un secondo certificato, con analoghe modalità di compilazione, che, a differenza del certificato ordinario, non è firmato dalla chiave privata della nuova coppia ma dalla chiave privata della coppia di chiavi in scadenza. Tale certificato è pubblicato secondo le modalità ordinarie nel registro dei certificati del Certificatore.

Viene inoltre emesso un certificato relativo alla coppia di chiavi in scadenza, firmato con la chiave privata della nuova coppia di chiavi.

17.2.3 Comunicazione - Registrazione presso il CNIPA

La copia dei tre certificati di cui al paragrafo precedente è fornita al CNIPA, che provvede all'aggiornamento della lista delle chiavi di certificazione contenuta nell'Elenco pubblico dei Certificatori tenuto dalla stessa Autorità ed al suo inoltro ai Certificatori per la pubblicazione.

18 Registro dei Certificati

18.1 Modalità di gestione

Nel Registro dei Certificati sono registrate le seguenti attività del Certificatore:

- pubblicazione dei certificati;
- sospensione dei certificati;

- riabilitazione dei certificati sospesi;
- revoca dei certificati.

La gestione del registro è attuata in conformità con le norme vigenti. In particolare, le registrazioni sono conservate per il periodo previsto dalla normativa in funzione della tipologia di registrazione e con le modalità richieste (art. 31, comma 6 del DPCM 2004).

Nel registro dei certificati sono presenti i seguenti elementi:

- i certificati emessi dal Certificatore, per la cui pubblicazione i titolari hanno espresso liberamente esplicito consenso;
- la lista dei certificati revocati;
- la lista dei certificati sospesi.

Il registro dei certificati è accessibile a qualsiasi soggetto, secondo le modalità previste dalla normativa e descritte nel capitolo 18.5 del presente Manuale Operativo. In particolare, si fa riferimento alle disposizioni seguenti:

- art. 29 bis, comma 2, lett. p del TUDA, Obblighi del titolare e del certificatore;
- art. 14, commi 3 e 4 del DPCM 2004;
- art. 27 del DPCM 2004, Requisiti di sicurezza dei sistemi operativi;
- art. 31 del DPCM 2004;
- art. 40 del DPCM 2004, comma 1, Obblighi per i certificatori accreditati.

18.2 Sicurezza

L'effettuazione delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato del Certificatore. In particolare, il Certificatore ha incaricato un Responsabile della gestione del Registro dei Certificati.

Tutte le attività di modifica del registro dei certificati sono opportunamente segnalate e archiviate dal Certificatore. Inoltre sono annotati i seguenti eventi relativi al registro:

- la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il registro dei certificati non risulta accessibile dall'esterno;
- ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

Il registro dei certificati è tenuto in doppia copia e almeno una copia di sicurezza della copia operativa e di quella di riferimento del registro dei certificati è conservata in armadi di sicurezza distinti, situati in locali diversi da quelli dei dispositivi tecnologici del Certificatore. L'integrità del giornale di controllo viene verificata mensilmente (art. 31, comma 5 del DPCM 2004).

18.3 Aggiornamento

Il registro dei certificati viene aggiornato ogni volta che viene emesso un certificato o una lista dei certificati sospesi o revocati.

18.4 Struttura della lista dei certificati revocati e sospesi

La lista dei certificati revocati e sospesi permette di pubblicare e distribuire liste di certificati revocati e sospesi.

Tale lista riporta i seguenti dati:

- data e ora di emissione;
- firma del Certificatore;
- elenco dei certificati revocati o sospesi, con la relativa motivazione;
- etichetta di status di ciascuno dei certificati inclusi (Revocato o Sospeso).

Inoltre, può essere consultata secondo le modalità descritte nel capitolo 18.5 del presente manuale.

La lista dei certificati revocati (CRL) o sospesi (CSL) è aggiornata in occasione di ogni nuova richiesta approvata di revoca, sospensione e riabilitazione.

La lista dei certificati revocati e sospesi è conforme allo standard X.509 CRL v2.

Si raccomanda di seguire scrupolosamente le indicazioni fornite al capitolo 20 per quanto attiene la corretta procedura di verifica della validità di una firma.

18.5 Modalità di Accesso e Consultazione

Le modalità di accesso al registro dei certificati sono stabilite in conformità con le norme vigenti.

Il registro dei certificati è pubblicato sotto forma di *directory*. L'accesso al registro avviene tramite protocollo LDAP, come definito dalla specifica pubblica RFC 1777 e successive modificazioni o integrazioni.

L'accesso avviene tramite rete Internet, all'indirizzo DNS riportato sul sito Web del Certificatore e nel paragrafo seguente, nonché nell'Elenco pubblico dei Certificatori tenuto dal CNIPA, ai sensi della normativa vigente.

18.6 Dati Identificativi del Registro

Il registro dei certificati può essere consultato mediante il protocollo (LDAP) collegandosi all'indirizzo: *ldap://ds.firmasicura.it*

19 Modalità operative per la generazione della firma digitale

In questo paragrafo vengono descritte, per linee generali, le modalità operative per la generazione della firma digitale (art. 38, comma 3, lett. t del DPCM 2004). Per un maggiore dettaglio sulle modalità operative in questione, si rinvia alla documentazione che viene consegnata agli utenti del servizio di firma digitale IT Telecom e che è disponibile per la consultazione sul sito www.firmasicura.it.

Ai sensi dell'art. 6, commi 4 e 5 del DPCM 2004, il Certificatore fornisce nel kit di utilizzo del servizio che consegna al Titolare un dispositivo sicuro per la generazione della firma digitale che è stato testato e per il quale è stata verificata la conformità alle normative vigenti (art. 29 sexies, commi 2 e 4 del TUDA; art. 3, comma 1 del DPCM 2004) e la perfetta compatibilità con le tecnologie utilizzate dal Certificatore nell'erogazione del servizio. In base al medesimo articolo, il titolare ha l'obbligo di utilizzare esclusivamente detto dispositivo fornito dal Certificatore.

Il Certificatore si riserva, inoltre, di verificare la compatibilità di dispositivi che i clienti o i titolari chiedessero di utilizzare in alternativa a quelli forniti o indicati dal Certificatore stesso.

Pertanto le operazioni di generazione della firma digitale da parte del titolare descritte nel seguito, si intendono effettuate mediante l'impiego di un dispositivo fornito dal Certificatore o da questi indicato o approvato.

19.1 Corretta rappresentazione dei documenti informatici

I documenti elettronici sono redatti mediante prodotti software di produttività individuale (elaboratori di testi, posta elettronica, fogli elettronici, elaboratori di immagini, ecc.). Alcuni di questi prodotti offrono architetture molto flessibili per il trattamento dei documenti stessi, consentendo l'inclusione di elementi multimediali, di collegamenti ipertestuali, di oggetti dinamici. Sebbene queste caratteristiche siano molto utili per le esigenze attuali dell'utenza, la rappresentazione sullo schermo dei documenti può essere notevolmente influenzata dal comportamento dei diversi elementi che li compongono, **rendendo di fatto aleatoria la visualizzazione da un contesto all'altro, anche se il file resta inalterato**.

Questi elementi di flessibilità prestano il fianco ad un uso malizioso: un utente esperto potrebbe facilmente inserire contenuti (macro, campi nascosti, ecc.) che alterano il documento, mostrando al suo interno informazioni dipendenti da file esterni o da diverse condizioni (ad esempio, una data o il risultato di un'operazione aritmetica), conducendo a **rappresentazioni molto diverse in momenti o contesti diversi**.

Ricordiamo in proposito che, affinché il documento informatico sottoscritto dal titolare con una firma digitale certificata dal Certificatore IT Telecom, generata mediante un dispositivo sicuro per la creazione di una firma, faccia piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto (art. 10, comma 3, del TUDA), **non deve contenere macroistruzioni o codici eseguibili, tali da attivare**

funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati (art. 3, comma 3 del DPCM 2004)[3].

Sono pertanto da ritenersi idonei a tale scopo e agli effetti sopra indicati tutti i documenti di tipo informatico derivanti da documenti elettronici in tutte le opzioni di programma che introducono forme di "**modificazione dinamica**" al contenuto del documento informatico[4] siano disattivate. Indipendentemente dal formato di un documento, è dunque indispensabile che il titolare al momento della firma o della verifica di un documento si accerti personalmente che nel documento non vi siano contenuti in grado di apportare **modificazioni dinamiche non desiderate**[5]. Per farlo, è opportuno fare riferimento alle istruzioni di uso dei programmi con i quali sono stati elaborati i documenti informatici, che chiariscono le caratteristiche dei formati di salvataggio e memorizzazione.

Ciò detto, è opportuno che il titolare tenga presenti le seguenti indicazioni:

- Il **rischio di ottenere una presentazione ambigua** dei dati è particolarmente elevato nel caso di documenti informatici basati su documenti elettronici composti da un elaboratore di testi, proprio a causa della natura di tali prodotti software, non progettati per ottenere visualizzazioni assolutamente univoche dello stesso documento in contesti diversi[6].
- Il Certificatore IT Telecom distribuisce, nell'ambito del proprio servizio di Certificazione della Firma Digitale il prodotto DigitalSign®, che visualizza i documenti di questo tipo in modo da **ridurre il rischio di alterazione dei dati durante la visualizzazione**. Nonostante questa funzionalità, per una effettiva analisi al fine di minimizzare i rischi, è altamente consigliabile configurare opportunamente il word processor.
- Per quanto concerne i **formati di salvataggio e memorizzazione dei documenti elettronici**[7] è opportuno tenere a mente quanto segue:
  - non utilizzare i **formati tipici** dei singoli strumenti software per i documenti particolarmente critici o nei casi in cui non si sia certi dell'affidabilità dell'autore del documento
  - usare con cura le funzionalità del prodotto software per analizzare il documento, alla ricerca di indicazioni della presenza o meno di campi di informazione sospetti (è utile consultare le **guide alla configurazione** dei singoli prodotti utilizzati)

19.2 Informazioni sui formati dei documenti

19.2.1 Il formato PDF

Il formato PDF (Portable Document Format) è stato progettato per l'interscambio di documenti in modo che il ricevente veda esattamente il documento come è stato creato, indipendentemente dalle diverse elaborazioni fatte su di esso. **È da considerare sicuro, se usato come base per documenti informatici firmati digitalmente, se la firma digitale è apposta/verificata tramite DigitalSign**.

[3] La deliberazione n. 51/2000 del 23 novembre 2000 dell'AIPA, prevede che I formati dei documenti informatici adottati dalla PA, possiedano almeno i requisiti di non alterabilità del documento durante le fasi di accesso e conservazione e di immutabilità nel tempo del contenuto e della sua struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto (art. 3, comma 1, lett. b) e d)).

[4] Si badi che, di fatto, quando si firma un documento informatico con questi contenuti, non si sta firmando un documento vero e proprio, ma un file di dati, che al suo interno, oltre a testi e/o grafici, contiene anche istruzioni in grado di alterare la natura del documento (ad esempio, aggiornamento automatico della data).

[5] Si fa riferimento, a puro titolo esemplificativo, ai campi aggiornabili automaticamente sia endogeni (una data, un'ora, numero di pagina, ecc.) sia esogeni come i riferimenti a documenti esterni a quello sottoscritto (richiamo del valore di una somma di un foglio di calcolo in un documento di test, ecc.)

[6] È facilmente ipotizzabile che la maggior parte dei documenti informatici si basi su testi scritti con tali programmi, altamente diffusi ed utilizzati.

[7] Il formato di un documento informatico (indicato da un'estensione di tre o quattro lettere che segue il nome del file stesso) definisce la modalità in cui vengono memorizzate le informazioni all'interno del file in modo tale che quest'ultimo possa essere aperto e salvato in un'applicazione.

19.2.2 Formati di Microsoft Office ®

Al momento non sono disponibili metodi certi per la verifica della presenza di tutti gli elementi in grado di alterare i contenuti del documento presentato tramite uno degli applicativi Microsoft Office ®. Pertanto, finché possibile, si sconsiglia l'uso dei formati **DOC**, **DOT**, **RTF**, **XLS**, per documenti particolarmente critici. Ove fosse indispensabile l'utilizzo di tali formati, prima di procedere alla sottoscrizione del documento è indispensabile **bloccare la "dinamicità" dei campi eventualmente presenti nel documento stesso** attivando le apposite istruzioni, oppure di trasferire i dati in altra forma (ad esempio, immagine) in un altro formato idoneo (ad esempio il sopra detto PDF).

Di seguito alcune informazioni specifiche sui principali formati Microsoft Word ® utili per la creazione di documenti informatici:

- **DOC** è il formato predefinito di un documento di Microsoft Word® e può contenere macro istruzioni.
- **DOT** è il formato di un modello di Microsoft Word® e contiene le istruzioni per l'applicazione della formattazione e degli attributi contenuti a tutti i nuovi documenti basati su tale modello.
- **RTF** (Rich Text Format) converte la formattazione in istruzioni che possono essere lette e interpretate da altri programmi e può contenere macro istruzioni.
- **TXT** non contiene informazioni sulla formattazione del testo e non consente l'utilizzo di macro istruzioni.
- **XLS** è il formato principale utilizzato da Microsoft Excel® per memorizzare ed elaborare dati mediante funzioni di varia natura.

19.2.3 Formati per le immagini

Vi sono numerosi formati disponibili per l'utilizzo di immagini come documenti elettronici. Fra questi si può distinguere tra:

- **formati non compressi** (o a bassa compressione), che vengono utilizzati per le applicazioni stand-alone, per la stampa o per conservare copie ad alta fedeltà di immagini.
- **formati compressi**, che generano documenti con dimensioni minori rispetto a quelli di partenza. A questo proposito è opportuno considerare che esistono due tipologie di compressione:
  - **senza perdita di dati**: la compressione è reversibile e dall'informazione compressa è possibile ricostruire esattamente l'informazione originale.
  - **con perdita di dati**: la compressione è irreversibile e non è più possibile ricostruire esattamente l'informazione originale.

Fra i formati non compressi o a bassa compressione (comunque senza perdita di dati) rientrano **BMP** (BitMaP - standard di Microsoft Windows® che permette compressioni senza perdita di dati) e **TIFF** (Tagged Image File Format - formato bitmap supportato da quasi tutte le applicazioni grafiche e molto utilizzato perché consente di scambiare file tra programmi e piattaforme diverse).

Tra i formati **compressi con perdita** si segnala il comune JPEG (Joint Photographic Experts Group), mentre tra quelli **compressi senza perdita**, il **GIF** (Graphic Interchange Format) ed il PNG (Portable Network Graphics).

Sebbene sul piano tecnico la compressione può essere visivamente impercettibile, **è opportuno evitare l'utilizzo di immagini sottoposte a procedimenti di compressione con perdita di dati** per la creazione di documenti informatici, preferendo in assoluto i formati non compressi o i formati compressi senza perdita. Per l'individuazione di queste caratteristiche, è opportuno fare riferimento alle specifiche informazioni fornite dal produttore del software utilizzato per il trattamento delle immagini o agli standard pubblicati dagli organismi competenti.

19.3 Generazione della firma digitale

La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui é apposta o associata; il Titolare, al momento della generazione della firma digitale deve accertarsi che il proprio certificato qualificato non risulti scaduto di validità ovvero non risulti revocato o sospeso (art. 23, commi 1 e 2 del TUDA).

L'apposizione di una firma digitale a un documento informatico avviene per mezzo di diversi strumenti matematici e si basa essenzialmente sulle seguenti operazioni:

- Dal documento viene calcolata un'impronta, tramite una funzione di HASH.
- L'impronta ottenuta viene crittografata con algoritmo asimmetrico RSA, utilizzando una chiave privata appartenente ad una coppia certificata da un fornitore di servizi di certificazione e contenuta all'interno di un dispositivo sicuro di firma.

Da un punto di vista operativo, la generazione della firma digitale prevede l'utilizzo di uno specifico prodotto applicativo.

Il Certificatore IT Telecom distribuisce a questo scopo *DigitalSign* ® – *Edizione IT Telecom*, che prevede due diverse modalità per apporre la firma digitale ad un documento:

- **creare *ex-novo* un documento e quindi sottoscriverlo**: una volta selezionata la tipologia di file desiderata tra quelle disponibili[8], il Titolare procederà alla stesura del documento che - una volta completato - potrà essere firmato digitalmente attraverso un'apposita funzionalità dell'applicativo. Naturalmente, se il documento viene ancora modificato dopo la firma, quest'ultima non sarà più valida (e *DigitalSign*® lo segnalerà)
- **apporre una firma digitale ad un documento preesistente**: l'utente aprirà un documento all'interno di *DigitalSign*® e procederà a sottoscriverlo digitalmente utilizzando un'apposita funzionalità dell'applicativo

In entrambi i casi, al momento di apporre la firma l'applicativo procederà per prima cosa a calcolare l'impronta (hash) del documento e quindi a crittografarla, utilizzando la chiave privata contenuta all'interno del dispositivo di firma del sottoscrittore.

Il risultato di questa operazione di crittografia è la firma digitale. I documenti informatici firmati digitalmente vengono organizzati in forma di file in formato PKCS#7, riconoscibili dall'estensione "p7m".

20 Modalità operative per l'utilizzo del sistema di verifica delle firme

Analogamente a quanto precisato nel paragrafo precedente, in questo paragrafo vengono descritte, per linee generali, le modalità operative per l'utilizzo del sistema di verifica delle firme digitali (art. 38, comma 3, lett. s del DPCM 2004). Per un maggiore approfondimento si rinvia alla documentazione specifica, disponibile sul sito www.firmasicura.it.

La verifica di una firma digitale è un'operazione estremamente delicata. Se la verifica della firma apposta a un documento ha esito positivo, difatti:

- si è certi che il documento non è stato modificato dal momento dell'applicazione della firma stessa;
- si è certi che il certificato del sottoscrittore è garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori, non è scaduto, sospeso o revocato ;
- l'autore della firma non potrà negare di averla emessa (non ripudio), a meno di intentare una querela di falso.

La verifica di una firma digitale può essere effettuata diverse tipologie di soggetti, con modalità differenti:

- titolari di un certificato di firma digitale IT Telecom Italia;
- titolari di un certificato di firma digitale di altro certificatore;
- soggetti che non dispongono del software fornito da un certificatore.

L'operazione di verifica **non richiede l'utilizzo di smartcard e lettore**, ma viene effettuata mediante un personal computer collegato ad Internet. Il collegamento occorre per la verifica dello stato del certificato, poiché i software di verifica si collegano alla lista di revoca pubblicata dal certificatore che ha emesso il certificato qualificato per rendere disponibili le informazioni relative alla sospensione o revoca del certificato.

Di norma, le operazioni suddette e più oltre descritte sono completamente automatiche, mentre deve essere effettuata manualmente la verifica dell'esistenza o meno di limiti di validità dipendenti dalla natura del

[8] Potranno essere utilizzati a tal fine gli applicativi che supportano la proprietà *Active Document*® (tipicamente le applicazioni di Microsoft Office®): queste applicazioni consentono infatti di generare un documento ex-novo e di editarlo all'interno della finestra documento di *DigitalSign* ®.

documento sottoscritto. Si tratta di una verifica estremamente importante, poiché **la sottoscrizione con firma digitale di un contratto al di fuori delle condizioni indicate nel certificato è considerata non valida, cioè corrisponde alla mancata sottoscrizione**. A titolo esemplificativo, rientra in questa casistica l'ipotesi di indicazione nel certificato di limiti di spesa entro i quali il titolare può sottoscrivere contratti che implichino transazioni monetarie. Tali annotazioni sono sempre incluse nel certificato relativo alla firma che si sta verificando.

20.1 Verifica della firma da parte di titolari di un certificato di firma digitale IT Telecom

Il titolare del certificato di firma digitale emesso da IT Telecom, per verificare la validità di una firma digitale apposta ad un documento potrà utilizzare l'applicativo *DigitalSign*®, contenuto all'interno del kit consegnato da IT Telecom.

La verifica della firma digitale viene effettuata automaticamente dall'applicativo, una volta che il file in questione[9] viene aperto in *DigitalSign*®. Al momento dell'apertura del file, difatti, l'applicativo compie una serie di passi:

1. *La firma digitale* viene decrittata utilizzando la chiave pubblica corrispondente alla chiave privata che era stata usata per generarla (crittografia asimmetrica RSA). Si ottiene in questo modo l'impronta da cui si era partiti. Chiamiamo "impronta decifrata" il risultato di questa operazione.
2. *Il documento originale* viene sottoposto alla stessa funzione HASH impiegata all'origine, ottenendo così la stessa impronta che aveva ricavato il sottoscrittore applicando tale funzione allo stesso documento. Chiamiamo "impronta calcolata" questo risultato.
3. L'impronta decifrata viene a questo punto confrontata con l'impronta calcolata: se esse coincidono allora la firma è autentica, perché né il documento né la firma sono stati alterati dal momento della firma.

L'esito positivo del confronto assicura l'integrità del documento e della firma, ma di per sé non assicura l'identità del sottoscrittore.

Poiché il certificato è firmato dalla Certification Authority che lo ha emesso, occorre controllare l'identità del sottoscrittore verificando la firma apposta a tale certificato. In pratica, si deve controllare la validità del certificato di chiave pubblica del certificatore che lo ha firmato.

L'applicativo, inoltre, verificherà la validità di ogni certificato digitale, andando a controllare nelle relative CRL (*Certificate Revocation List*) che questi non siano scaduti, sospesi o revocati[10].

Da un punto di vista operativo, ricordiamo che DigitalSign® – IT Telecom Edition compie tutte queste verifiche in modo automatico: l'esito di tali verifiche verrà evidenziato all'interno di una finestra che compare al momento dell'apertura del documento.

20.2 Verifica della firma da parte di titolari di un certificato di firma digitale di altro certificatore

Il titolare del certificato di firma digitale emesso da un certificatore iscritto nell'Elenco Pubblico del CNIPA diverso da IT Telecom, può verificare la validità di una firma digitale apposta ad un documento utilizzando

[9] Ricordiamo che il documento firmato è un vero e proprio documento informatico, rappresentato da un file in formato PKCS#7. Tale file contiene, nel caso più semplice possibile:

• Il documento elettronico originale in forma integrale

• La firma digitale relativa al documento

• Il certificato della chiave pubblica la cui corrispondente chiave privata è stata usata per generare la firma.

[10] È opportuno ricordare che un documento con firma digitale scaduta o revocata è valido solamente se al documento è possibile associare un riferimento temporale opponibile ai terzi (ad esempio, una marca temporale rilasciata da un Certificatore iscritto nell'Elenco Pubblico dei Certificatori), apposta durante il periodo di validità del certificato della firma. Va da sé che si tratta solo di un'indicazione generale; i casi devono essere esaminati in specie e tenendo presenti anche concetti più generali che riguardano campi più ampi di quello della sola firma digitale.

l'applicativo messo a disposizione dal proprio certificatore, oppure le modalità previste al paragrafo successivo per chi non dispone del software fornito da un certificatore.

20.3 Verifica della firma da parte di soggetti che non dispongono di un software di verifica fornito da un certificatore

I soggetti che hanno la necessità di verificare una firma digitale, ma non dispongono di un software specifico possono effettuare l'operazione utilizzando l'applicativo messo gratuitamente a disposizione sui siti www.firmasicura.it oppure www.comped.it.

In alternativa, possono fare riferimento ai software freeware indicati dal CNIPA sulle *Linee guida per l'utilizzo della firma digitale* e pubblicati sul sito www.cnipa.gov.it .

PARTE IV

Marcatura Temporale

21 Riferimento Temporale

I certificati relativi a chiavi di marcatura temporale sono assoggettati alla medesima regolamentazione dei certificati relativi a chiavi di sottoscrizione. In tal caso, il titolare del certificato è il responsabile del servizio di marcatura temporale che ne fa uso.

Per quanto riguarda le attività sotto elencate si fa quindi riferimento ai paragrafi del presente Manuale Operativo indicati:

- Generazione delle chiavi, par. 13.1;
- Tipologia e struttura dei certificati, par. 14.1;
- Generazione e pubblicazione dei certificati, par. 14.2;
- Sostituzione delle chiavi, par. 17.1.

In base a quanto previsto dal DPCM 2004, il Certificatore redige un giornale di controllo contenente le registrazioni effettuate automaticamente dai dispositivi installati, garantendo che a ciascuna registrazione venga associato un riferimento temporale per la sua opponibilità verso terzi. L'ora assegnata a ciascun riferimento corrisponde alla scala di tempo UTC (IEN) con una differenza non superiore al minuto primo (art. 31, comma 1 e 3 ed art. 39, comma 2 e 3 del DPCM 2004).

Il Certificatore garantisce l'autenticità delle annotazioni contenute nel suddetto giornale di controllo, così come la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza. Il Certificatore verifica con cadenza mensile l'integrità del giornale ed assicura la conservazione delle registrazioni in esso contenute per un periodo di tempo non inferiore ai dieci anni (art. 31, comma 4, 5, e 6 del DPCM 2004).

Si evidenzia che tutti i sistemi del centro servizi IT Telecom sono periodicamente allineati con i suddetti riferimenti temporali tramite comandi opportunamente configurati e schedulati sui sistemi stessi.

22 Validazione Temporale

In questo capitolo si descrivono le modalità di utilizzo del servizio di Validazione Temporale del Certificatore IT Telecom.

Il servizio è il risultato di una procedura informatica che attribuisce ad uno o più documenti informatici un riferimento temporale opponibile ai terzi, associando a qualsiasi evidenza informatica (intesa come sequenza di simboli binari) una data ed un'ora certe, validando temporalmente queste informazioni, mediante la generazione di una marca temporale (art. 1, comma 1, lett. f), g), h), i) e art. 44, comma 1 del DPCM 2004).

Per marca temporale si intende una struttura di dati (ovvero l'impronta del documento cui la marca si riferisce, ottenuta attraverso un'apposita funzione di hash) firmata digitalmente, così da poter attribuire al documento informatico in oggetto un riferimento temporale (data ed ora) sicuro e verificabile (art. 1, comma 1, lett. d ed e del DPCM 2004).

Ciascuna marca generata ed apposta su un documento informatico è indissolubilmente legata al documento stesso grazie a riferimenti certi, quali:

- l'**impronta del documento** (con l'indicazione dell'algoritmo impiegato) che rende univoca l'associazione dello stesso con la marca temporale;
- il **numero progressivo** seriale della marca che ne sancisce la esclusività della marcatura;
- **la data e l'ora** relative alla richiesta dell'utente al Certificatore.

Tramite il servizio di validazione temporale, gli utenti possono associare un riferimento temporale ai propri documenti elettronici e quindi dimostrare la loro esistenza, dando loro validità legale, con l'utilizzo congiunto della firma digitale. Grazie al servizio, l'utente può:

- apporre una marca temporale ad un qualsiasi documento informatico (art. 44, comma 1 del DPCM 2004);
- estendere la validità legale di un documento firmato digitalmente nel tempo, oltre il periodo di validità del certificato di sottoscrizione medesimo (art. 52 del DPCM 2004);
- verificare la validità delle marche temporali presenti su documenti informatici in suo possesso.

In base alle richieste dell'utente, ciascuna marca temporale viene generata e firmata da un apposito sistema elettronico sicuro (TSA – *Time Stamping Authority*) del Certificatore IT Telecom, così da dimostrare l'esistenza del documento informatico, mediante il riferimento temporale indicato nella marca associata al documento stesso (art. 44, comma 2 del DPCM 2004).

22.1 Richieste di emissione o verifica di marche temporali

L'utente invia le proprie richieste di emissione o di verifica di marche temporali al sistema elettronico del Certificatore (TSA) avvalendosi di appositi applicativi software. Il Certificatore genera le marche richieste con 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. 48, comma 1 ed art. 51, comma 5 del DPCM 2004).

Per ciascuna evidenza informatica il Certificatore prevede l'emissione di una sola marca temporale associata (art. 51, comma 2 e 4 del DPCM 2004).

22.1.1 Richiesta di emissione tramite applicativo client di firma e verifica

Mediante l'applicativo client per la firma digitale e verifica della firma di documenti informatici (DigitalSign IT Telecom Edition), l'utente può inviare direttamente al server TSA del Certificatore le richieste di emissione di marche temporali (o verifica delle stesse) che contengono una evidenza informatica del documento a cui le stesse devono far riferimento. La Time Stamping Authority del Certificatore genera le marche e le rinvia al client dopo aver effettuato i più opportuni controlli circa le credenziali del richiedente e la correttezza della richiesta.

22.1.2 Richiesta di emissione via Web

Per garantire anche via web l'associazione di un riferimento temporale ad un qualsiasi documento informatico, l'utente seleziona il file relativo al documento da marcare, mediante un'applicazione software inviatagli dal sistema del Certificatore. In questo modo, è possibile calcolare l'impronta del documento localmente, senza che lo stesso venga inviato al server, per assicurarne la riservatezza. Una volta preparata la richiesta, tramite la medesima applicazione, l'impronta viene inviata alla Time Stamping Authority del Certificatore. A questo punto, il server TSA applica la marca temporale e firma la richiesta mentre l'applicazione localmente genera per l'utente un file con lo stesso nome dell'originario ed estensione *MIME*, contenente il file originario e la marca temporale ad esso associata.

22.1.3 Richiesta di verifica di marche temporali

Indifferentemente dal sistema impiegato (applicativo client o web), l'utente può richiedere la verifica di una marca temporale associata:

- ad un file con estensione MIME (contenente il documento originario e la marca temporale ad esso associata), oppure
- al documento originale, purché la marca sia in formato "Time Stamp Response".

La procedura di accertamento predisposta dal Certificatore consente di verificare sia la firma della TSA, attraverso la chiave pubblica cui corrisponde la chiave privata impiegata per la generazione della marca, che il valore dell'impronta del documento contenuto nella marca, attraverso il confronto con il valore dell'impronta inviato in fase di richiesta alla stessa TSA.

22.2 Emissione o verifica di marche temporali

In base alle diverse procedure e modalità previste dal Certificatore, alla ricezione delle richieste inviate dagli utenti del servizio di validazione temporale, il sistema elettronico TSA genera e firma in maniera automatica, dopo gli opportuni controlli, le marche temporali associate ai documenti informatici cui si richiede un riferimento temporale preciso e sicuro (data ed ora) corrispondente al Tempo Universale Coordinato (UTC), assieme a tutte le altre informazioni contenute nella marca (art. 48, comma 1 e 2 del DPCM 2004).

Attraverso un apposito algoritmo di hash SHA-1, definito nella norma ISO/IEC 10118-3:1998 come dedicated hash - function 3 (art. 51, comma 3 del DPCM 2004), l'utente può calcolare con il suo applicativo client o via web l'impronta relativa all'evidenza informatica da sottoporre a validazione temporale ed inviare la sua richiesta alla Time Stamping Authority del Certificatore. Successivamente, il server TSA provvede alla

generazione della marca temporale che contiene una serie di informazioni (art. 45, comma 1 e 2 del DPCM 2004), tra cui:

- l'impronta del documento (con l'indicazione dell'algoritmo impiegato) che rende univoca l'associazione dello stesso con la marca temporale;
- il numero progressivo seriale della marca che ne sancisce la esclusività della marcatura;
- la data e l'ora relative alla richiesta dell'utente al Certificatore.

La procedura di validazione ha termine con la firma della TSA alla struttura dei dati così generata e l'invio della stessa marca all'utente richiedente.

22.3 Generazione delle chiavi di marcatura temporale della TSA

Il responsabile del sistema di riferimento temporale del Certificatore è l'unico soggetto abilitato alla generazione delle chiavi di marcatura temporale impiegate per la sottoscrizione dei relativi certificati (art. 46, comma 3 e 4 del DPCM 2004). Ciascuna coppia di chiavi della TSA del Certificatore ha validità annuale ed è generata all'interno di un apparato hardware crittografico (HSM – *Hardware Security Module*), utilizzando l'algoritmo asimmetrico RSA con chiavi non inferiori a 1.024 bit di lunghezza e sostituita ogni mese, al fine di limitare il numero delle marche generate con la medesima coppia, senza revocarne il corrispondente certificato (art. art. 46, comma 1 e 2 del DPCM 2004).

Per la verifica di tutte le marche generate dalla TSA, il Certificatore IT Telecom emette un certificato di chiave pubblica della TSA che pubblica in un apposito registro dei certificati, così da renderlo disponibile a tutti gli utenti. Al fine di garantire l'autenticità e l'integrità della chiave pubblica impiegata, la corrispondente chiave privata viene memorizzata nell'apparato crittografico, così da impedirne l'esportazione e l'uso improprio.

Si evidenzia, inoltre, l'impiego esclusivo della coppia di chiavi così generata per la certificazione delle chiavi delle marche temporali emesse, in quanto i certificati per i Titolari di chiavi di sottoscrizione sono firmati con una diversa coppia di chiavi (art. 4, comma 4 e 5 del DPCM 2004).

22.4 Marche Temporali

Tutti i certificati emessi dal Certificatore sono conformi alle "Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico"[11] e contengono l'identificativo del sistema di marcatura temporale che utilizza le chiavi relative (art. 47, comma 1 e 2 del DPCM 2004).

In coerenza con la normativa vigente, il Certificatore si è basato sulle specifiche tecniche esposte dal gruppo di lavoro dello IETF (Request for Comment 3161), relativo alle tematiche legate all'infrastruttura PKI ed al protocollo di comunicazione TSP (Time Stamp Protocol) con la TSA, per definire il formato delle marche temporali nell'ambito del suo servizio di Validazione Temporale.

Riguardo al contenuto delle stesse marche temporali, di seguito si riportano tutte le informazioni presenti nei relativi certificati (art. 45, comma 1 del DPCM 2004):

a) identificativo della CA emittente: IT Telecom Time Stamp Authority;
b) numero di serie della marca;
c) algoritmo impiegato per la sottoscrizione della marca: RSA;
d) identificativo del certificato relativo alla chiave pubblica di verifica della marca;
e) data ed ora di generazione della marca;
f) identificatore dell'algoritmo di hash impiegato per la generazione dell'impronta dell'evidenza informatica sottoposta a validazione temporale;
g) valore dell'impronta dell'evidenza informatica.

22.4.1 Registrazione delle marche temporali

Il sistema di Validazione Temporale del Certificatore IT Telecom garantisce la conservazione di tutte le marche temporali emesse in un apposito archivio digitale non modificabile, per un periodo non inferiore ai

[11] Si veda la Circolare n. AIPA/CR/24 del 19 giugno 2000, che ha recepito le norme tecniche internazionali per la firma digitale, contenute nella ISO/IEC 9594-8:2001

cinque anni. Su richiesta dell'interessato, è possibile conservare le suddette marche per un periodo maggiore, secondo specifiche condizioni previste dal Certificatore medesimo (art. 50, comma 1 del DPCM 2004).

22.4.2 Validità delle marche temporali

Una marca temporale ha validità sino alla scadenza del certificato ad essa associato e per l'intero periodo della sua conservazione nell'apposito archivio del Certificatore (art. 50, comma 2 del DPCM 2004).

Il certificato di marcatura temporale di IT Telecom ha una durata di cinque anni. Tuttavia, possono essere concordati con gli utenti periodi di validità maggiori. In alternativa, prima della scadenza del certificato, può essere associata una nuova marca all'evidenza informatica relativa alla marca precedente, così da dare continuità alla validità del documento originario.

Si ricorda che, per estendere nel tempo l'efficacia legale di un documento informatico firmato digitalmente, è sufficiente associare successivamente al medesimo documento nuove marche temporali (art. 52 del DPCM 2004).

22.5 Sicurezza del sistema di Validazione Temporale

Personale espressamente autorizzato dal certificatore provvede al buon funzionamento del servizio di validazione Temporale, attraverso un sistema di monitoraggio interno che consente il controllo continuo delle fonti di riferimento temporale, verificando lo stato dei server presenti nel Centro Servizi del Certificatore. Mediante un dispositivo denominato TIME CHECK, infatti, è possibile richiedere, tramite protocollo SMNP, il riferimento temporale all'elemento di rete monitorato (server), confrontando i dati ricevuti con quelli del sistema di monitoraggio, sincronizzato con una terza parte esterna, lo IEN "Galileo Ferraris".

Il personale del Certificatore analizza eventuali anomalie accorse al servizio di Validazione Temporale, registrate automaticamente in un apposito registro operativo su di un supporto non riscrivibile (art. 49, comma 1 e 2 del DPCM 2004), come:

- asincronismo con la fonte esterna di riferimento (IEN);
- differenza oraria maggiore o uguale ad un minuto primo;
- indisponibilità o manomissione del supporto non riscrivibile;
- tentativo di sabotaggio del sistema.

Al verificarsi dei suddetti accadimenti, il personale autorizzato provvede al blocco del sistema, prima della sua pronta risoluzione (art. 49, comma 3 del DPCM 2004).

Si ricorda, inoltre, la conformità del sistema di Validazione Temporale del Certificatore ai requisiti di sicurezza previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC (art. 49, comma 4 del DPCM 2004).

PARTE V

Carta Nazionale dei Servizi

23 Soggetti coinvolti nel processo di emissione della CNS

I soggetti coinvolti nel processo di emissione delle carte sono:

- L'**Ente Emettitore**: è la Pubblica Amministrazione che emette le CNS.
- L'**Ente Certificatore**: il soggetto che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche e che, in conformità con le norme sulla CNS, genera per l'Ente Emettitore i certificati di autenticazione CNS.
- Il **Produttore delle Carte**: il soggetto che provvede alla fornitura delle smartcard, che predispone opportunamente gli spazi dedicati alla carta sanitaria (Netlink) ed alla firma digitale, che applica al supporto fisico l'artwork e gli altri elementi costanti.

Di seguito sono indicate le attività che le Linee Guida assegnano a ciascuno dei tre soggetti.

È opportuno osservare che le attività riconducibili ai ruoli sopra identificati sono separate solo a livello teorico: **da un punto di vista operativo possono essere svolte da uno o più soggetti, a prescindere dal ruolo di pertinenza (par. 2.2.4 delle LG CNS)**.

23.1 Ente Emettitore

Le attività di **esclusiva pertinenza e responsabilità dell'Ente Emettitore** sono:

- **registrazione ed identificazione dei cittadini utenti**;
- **aggiornamento dell'Indice Nazionale delle Anagrafi**: prima di personalizzare la CNS, l'ente emettitore verifica i dati identificativi ed aggiorna l'Indice Nazionale delle Anagrafi, direttamente o tramite struttura delegata, mediante i servizi del sistema informativo del Ministero dell'Interno – Centro Nazionale dei Servizi Demografici.

Le attività che seguono possono invece essere **delegate dall'Ente Emettitore**, che tuttavia ne mantiene la responsabilità:

- **Personalizzazione della CNS**: inserimento delle informazioni utente necessarie per l'identificazione in rete e nella generazione dei codici PIN e PUK, utilizzabile per lo sbocco della carta nel caso di iterata digitazione errata del PIN;
- **Consegna della CNS**: recapito della CNS e della busta oscurata contenente PIN e PUK al titolare, previa verifica dell'identità.
- **Formazione del Titolare**: comunicazione delle modalità di uso della carta e delle procedure da utilizzare in caso di anomalie o disservizi
- Attivazione di un canale di **comunicazione telefonica** per richieste di sospensione o revoca.
- **Gestione della carta**: l'ente emettitore deve gestire le CNS emesse predisponendo le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza. Deve inoltre provvedere al ritiro della CNS alla scadenza e in occasione di malfunzionamenti.

L'Ente Emettitore è tenuto al rispetto di caratteristiche di qualità e di affidabilità tali da garantire la sicurezza dell'intero circuito (par. 2.2.7 dell LG CNS) e deve, quindi:

- rispettare le specifiche di qualità previste dalla norma ISO 9000/2000;
- soddisfare i requisiti di sicurezza del circuito della CNS (cap. 11 delle LD CNS);
- garantire affidabilità e sicurezza nelle modalità di interazione con i produttori delle carte e con gli enti certificatori;
- predisporre un **manuale operativo** che evidenzi le procedure seguite per la gestione di tutte le fasi del processo di emissione e di gestione della CNS;
- predisporre un **manuale utente** che illustri le modalità d'uso della CNS, i modi per usufruire dei servizi in rete e le procedure da seguire in caso di smarrimento, furto o compromissione della carta;
- organizzarsi in modo da costituire il riferimento per ogni problema di funzionalità, disponibilità o sicurezza del circuito di emissione, rendendo disponibile un recapito telefonico costantemente attivo;
- predisporre il **piano della sicurezza** relativo all'intero circuito di emissione.

Come accennato in precedenza, l'Ente Emettitore può delegare a terzi tutte le funzioni di emissione della CNS o di parte di esse, purché questi assicurino il rispetto dei requisiti sopra elencati.

23.2 Ente Certificatore

L'Ente Certificatore è responsabile della generazione del certificato di autenticazione sulla base delle informazioni anagrafiche ottenute dall'Ente Emettitore nella fase di registrazione.

I certificati di autenticazione della CNS possono essere emessi esclusivamente da Certificatori Accreditati, che devono attenersi alle norme che regolano l'emissione e la gestione dei certificati qualificati.

Tutti i certificatori che rilasciano certificati di autenticazione CNS devono essere iscritti in un elenco consultabile in via telematica, tenuto dal Dipartimento per l'Innovazione e le Tecnologie.

23.3 Produttore delle carte

Il produttore delle carte è responsabile della produzione del supporto fisico della CNS, della relativa inizializzazione tramite la generazione del file system, e della creazione delle condizioni necessarie per controllare l'accesso ai file. L'operazione di inizializzazione è finalizzata a produrre in maniera sicura delle carte che siano pronte ad essere personalizzate, ossia risultino in uno stato definito "Attivate".

I requisiti cui i Produttori delle carte devono rispondere sono fissati dal par. 2.2.7 delle LG CNS. In particolare, nella produzione delle carte dovranno essere rispettate le specifiche del sistema operativo (APDU) e della struttura interna della carta (file system) pubblicate sul sito del CNIPA.

24 Caratteristiche del servizio di CNS di IT Telecom

In qualità di Certificatore Accreditato per l'emissione di certificati qualificati di firma digitale, il Certificatore IT Telecom, in relazione ai ruoli, alle attività e alle responsabilità indicate nell'ambito della CNS dalla normativa vigente, può effettuare le attività associate ai seguenti ruoli e precedentemente sintetizzate:

- Ente Emettitore, **limitatamente alle attività di personalizzazione, consegna e gestione delle CNS**;
- Ente Certificatore;
- Produttore delle Carte.

Il servizio è fornito alle Pubbliche Amministrazioni titolate ad emettere le CNS con le modalità descritte nel seguito, in funzione delle esigenze specifiche e delle richieste delle Pubbliche Amministrazioni stesse.

24.1 Supporto della CNS

Da un punto di vista strutturale la CNS è una smartcard opportunamente configurata, contenente un certificato elettronico per l'autenticazione in rete del titolare.

Oltre a garantire funzionalità di autenticazione la CNS prodotta dal Certificatore IT Telecom è idoneamente predisposta già dal momento dell'emissione per:

- operare come **carta sanitaria**;
- ospitare il servizio di **firma digitale** (cap. 7 delle LG CNS).

Conformemente a quanto definito dalla disciplina vigente, la CNS reca impresso sul dorso la dicitura **Carta Nazionale dei Servizi** ed il nome della Pubblica Amministrazione che l'ha emessa. Inoltre, non presenta elementi di identificazione a vista del Titolare (ad esempio una fotografia) che possano farla confondere con una Carta di Identità Elettronica.

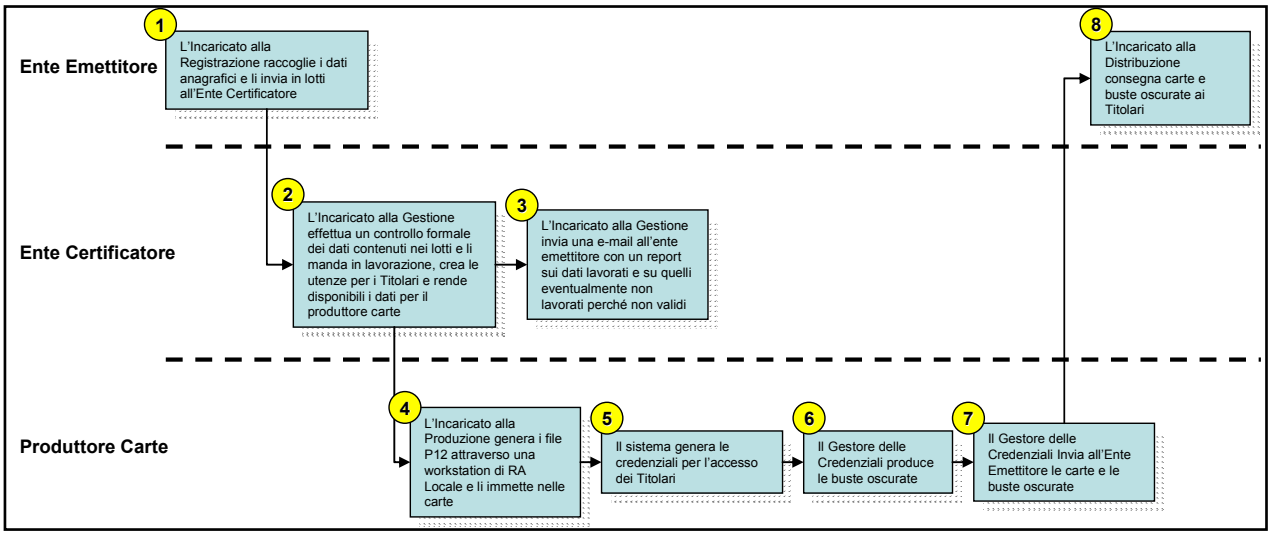
Per quanto riguarda le caratteristiche della carta, il Certificatore IT Telecom garantisce che:

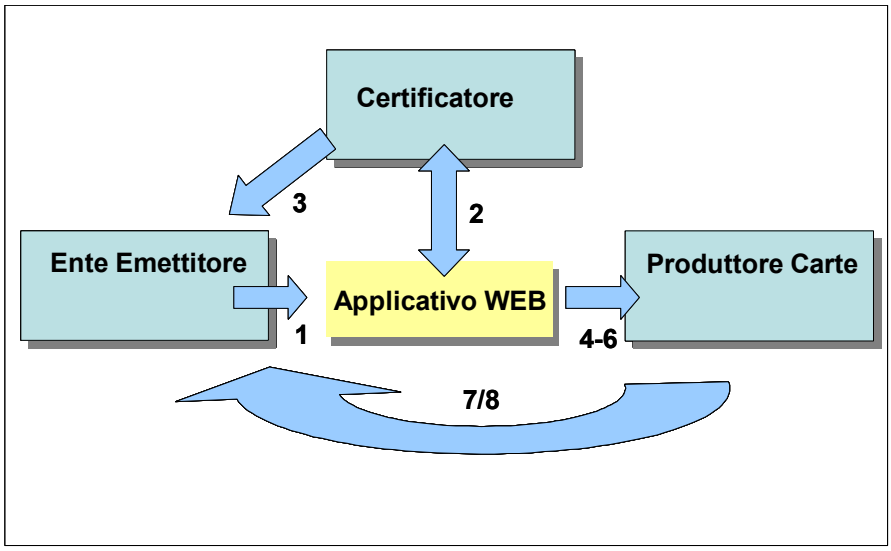
- il supporto fisico rispetta tutti i vincoli imposti dagli standard internazionali delle smartcard. In particolare, dimensione, spessore e tolleranze sono conformi a quanto specificato dalla norma ISO/IEC 7810: 1985 per la carta di tipo ID-1;
- è presente una memoria EEPROM di capacità uguale o superiore a 32Kb;
- il microprocessore è conforme agli standard ISO/IEC 7816;

- in aggiunta a quanto prescritto dallo standard ISO/IEC 7816 parte 4, 8, 9 e 10 circa i comandi del sistema operativo, sono rispettate le specifiche del sistema operativo (APDU) oggetto del protocollo d'intesa per la realizzazione dei progetti Carta d'Identità Elettronica e Carta nazionale dei servizi (P.d.I. 13 maggio 2003).

24.2 Modalità operative del servizio

In questo paragrafo viene descritta l'articolazione del processo di emissione delle CNS di IT Telecom. Lo schema rappresentato nella figura qui sotto illustra sinteticamente le diverse fasi del processo. Fatta eccezione per la fase 1 - che non può essere delegata dalla Pubblica Amministrazione che ricopre il ruolo di Ente Emettitore - IT Telecom è in grado di gestire tutte le altri fasi individuate.





Il processo comprende una serie di attività di pertinenza dei tre Ruoli teorici individuati. All'interno di ciascuno di detti ruoli sono individuate le seguenti figure:

- **Ente Emettitore:**
  - Incaricato alla Registrazione;
- **Ente Certificatore:**
  - Incaricato alla Gestione;
- **Produttore delle Carte:**
  - Incaricato alla Produzione;
  - Gestore delle Credenziali.

In relazione alla specifica configurazione del servizio, tali figure possono appartenere a diverse organizzazioni. IT Telecom procede all'identificazione di tutte le figure esterne che rappresentano un'interfaccia rispetto alle fasi presidiate direttamente. L'identificazione di tali figure segue modalità analoghe a quelle previste per gli incaricati dell'identificazione nell'ambito del servizio di certificazione della firma digitale (cap. 12). Tali soggetti operano utilizzando i sistemi, le procedure ed i certificati di autenticazione messi a disposizione da IT Telecom.

Fase 1 L'Incaricato alla Registrazione dell'Ente Emettitore procede alla **verifica dell'identita dei Titolari** e alla **registrazione dei dati dei Titolari** su schede anagrafiche. Per svolgere questa attività, l'Incaricato alla registrazione utilizza un apposito applicativo fornito da IT Telecom che garantisce autenticazione, riservatezza ed integrità dei dati forniti. Una volta raccolte le schede anagrafiche dei Titolari le trasferisce in lotti di massimo 5.000 unità al Certificatore.

I dati trasmessi per la generazione del certificato sono:

- Numero Seriale Smart Card (identifica una richiesta in modo univoco e la sua corretta associazione ad una specifica carta precedentemente confezionata);
- Nome;
- Cognome;
- Codice Fiscale;
- Data di Inizio Validità di Carta/Certificato (in formato aaaammgg);
- Data Fine Validità di Carta/Certificato (in formato aaaammgg);
- File dei dati personali (così come inserito nella smartcard).

Fase 2 L'Incaricato della Gestione effettua un **controllo formale sulle schede anagrafiche** inviate dall'Ente emettitore e predispone le utenze dei Titolari utilizzando un apposito applicativo. A questo punto i dati anagrafici sono resi disponibili in modalità sicura al Produttore delle Carte per la successiva lavorazione.

Fase 3 L'Incaricato della Gestione invia all'Ente Emettitore un *report* con la specifica delle schede anagrafiche sulle quali la lavorazione è stata effettuata e di quelle eventualmente non lavorate, ad esempio in caso di incongruenze nei dati registrati nella prima fase.

Fase 4 L'Incaricato alla Produzione delle carte avvia la sua lavorazione utilizzando un'apposita work station. Per ogni Titolare registrato viene generato un file P12 che verrà installato sulla rispettiva carta.

Fase 5 Il sistema genera automaticamente le credenziali per l'accesso al servizio di ciascun titolare e le cifra con la chiave pubblica del Gestore delle Credenziali.

Fase 6 Il Gestore delle Credenziali stampa le credenziali indicate al punto precedente all'interno di una busta oscurata.

Fase 7 L'Incaricato alla Produzione delle carte invia i plichi contenenti le carte e quelli contenenti le buste oscurate. Ogni consegna di lotti di CNS all'Ente Emettitore è accompagnata da una distinta, con la specifica del numero di CNS inizializzate e l'elenco dei relativi numeri seriali.

In sintesi per ogni richiesta del lotto vengono effettuate le seguenti operazioni:

- determinazione della policy Unicert da applicare (template di certificato);
- generazione di una coppia di chiavi RSA a 1024 bit;
- emissione del certificato di autenticazione;

- estrazione del Serial Number della carta del certificato emesso;
- generazione di una password per il file PKCS#12;
- produzione di un file PKCS#12 contenente le chiavi e i certificati, protetto mediante la password del punto precedente;
- memorizzazione su una partizione protetta del file system del file PKCS#12;
- aggiornamento dello stato della richieste e del lotto sul database.

24.3 Sospensione, Revoca e Riemissione della CNS

La validità temporale di una carta nazionale dei servizi viene fissata dall'Ente Emettitore al momento della predisposizione del servizio, in ogni caso, sulla base delle disposizioni contenute nel DPR 117/2004, la validità non può essere superiore a sei anni.

La validità di una CNS può decadere anche prima della sua scadenza naturale nei casi seguenti:

- smarrimento;
- furto;
- variazione dei dati anagrafici del titolare ai sensi dell'articolo 8, comma 4, del DPR 2 marzo 2004, n.117;
- revoca su iniziativa l'ente emettitore, fatto salvo l'obbligo di avvertire il titolare e di spiegarne le motivazioni.
- malfunzionamento o deterioramento del dispositivo.

In tutti questi casi la CNS potrà essere riemessa, su richiesta del Titolare, ma dovrà in ogni caso essere preventivamente ritirata da parte dell'Ente Emettitore di riferimento.

Le modalità tecniche con cui si effettuano revoca e sospensione delle CNS sono analoghe a quelle previste nel caso dei certificati di firma digitale, descritte in precedenza.

IT Telecom mette a disposizione dei Titolari delle CNS:

- un servizio di sospensione via portale web delle carte;
- un servizio telefonico di sospensione delle carte, con disponibilità analoga a quello previsto per i certificati di firma digitale.

24.4 CRL

Ogni certificato non scaduto, se revocato o sospeso viene inserito in una lista dei certificati revocati detta CRL. La sospensione può essere annullata ed il certificato rimosso dalla CRL, mentre la revoca è una operazione definitiva. I certificati revocati o sospesi vengono comunque rimossi dalla CRL al termine del loro periodo di validità.

In considerazione dell'elevato numero dei certificati da emettere, le modalità di pubblicazione della CRL sono tali da consentire alle applicazioni una ragionevole velocità nella consultazione della stessa. Le CRL emesse hanno uno *scope* limitato ad un certo insieme di certificati emessi (ad es. una CRL diversa per un determinato numero di certificati).

La pubblicazione delle CRL avviene ad intervalli prefissati e non prevede l'emissione di CRL estemporanee. La frequenza di pubblicazione della CRL dipende dalla numerosità dei certificati emessi dalla CA e comunque non è superiore alle 24 ore.

Le CRL sono pubblicate su un directory server (X.500) e accessibili a chiunque in forma anonima mediante protocollo standard LDAP (v2 e v3). L'indirizzo completo dal quale ottenere la CRL è contenuto all'interno del singolo certificato, valorizzato nell'estensione "standard CRL Distribution Point".

24.5 Chiavi di Certificazione

24.5.1 Caratteristiche della CA

Nel seguito vengono descritte le caratteristiche delle chiavi di certificazione e dei certificati relativi prodotti per le CA di Produzione.

Le chiavi della CA CNS hanno le seguenti caratteristiche:

Algoritmo	RSA
Lunghezza chiavi	2048

Il certificato emesso in associazione alle chiavi di certificazione è di tipo self-signed ed è stato emesso con le seguenti caratteristiche:

versione X.509	3
numero di serie	1 (0x01)
Issuer DN	C=IT, O=I.T. Telecom S.R.L., OU=Servizi di certificazione, CN=I.T. Telecom CNS CA
Subject DN	C=IT, O=I.T. Telecom S.R.L., OU=Servizi di certificazione, CN= I.T. Telecom CNS CA
Validità temporale	12 anni
Algoritmo firma	sha1-RSA
Estensioni X.509v3	
basicConstraints	CA, Path Lenght=0, CRITICA
keyUsage	Certificate Signing, CRL Signing, CRITICA
subjectKeyIdentifier	Hash SHA-1(160 bits) della chiave pubblica della CA (esadecimale) NON CRITICA
certificatePolicies	OID=1.3.76.12.1.1.5 URI= https://www.tipki.it/CACNS/CPS, NON CRITICA

24.5.2 Caratteristiche delle chiavi e dei certificati per i titolari

Le chiavi di autenticazione ed i relativi certificati per i titolari hanno le seguenti caratteristiche:

Algoritmo	RSA
Lunghezza chiavi	1024

Il certificato emesso in associazione alle chiavi di autenticazione è conforme alle specifiche tecniche relative riportate nel Regolamento Tecnico relativo alla Carta Nazionale dei Servizi.
Il certificato è emesso direttamente dalla CA e con le seguenti caratteristiche:

versione X.509	3
Issuer DN	C=IT, O=I.T. Telecom S.R.L., OU=Servizi di certificazione, CN=I.T. Telecom CNS CA
Subject DN[12]	C=IT, O='nome_convenzionale del progetto', OU='nome della PA Emittente', CN='codice fiscale'/'seriale della carta'.'hash dei dati personali'
Validità temporale	(5 anni)
Algoritmo firma	Sha1-RSA

[12] La struttura del DN qui riportata è da intendersi a titolo esemplificativo, potendo variare, compatibilmente alla normativa vigente, in funzione delle richieste degli Enti Emettitori.

Estensioni X.509v3	
keyUsage	Digital Signature (bit 0), CRITICA
extendedKeyUsage	TLS WWW Client Autentication, NON CRITICA
subjectKeyIdentifier	Hash SHA-1(160 bits) della chiave pubblica del titolare (esadecimale)= 1F944CBD67979DD64EF0AE8CFF9C9C04948EBD11, NON CRITITCA
authorityKeyIdentifier	Hash SHA-1(160 bits) della chiave pubblica della CA (esadecimale)= 3F949CB266979DD64EF08E8CFD9C9C04948EED15, NON CRITICA
certificatePolicies	OID= 1.3.76.12.1.1.10.2.2.11, URI= https://www.tipki.it/CNSCA/CPS, NON CRITICA
crlDistributionPoints	URI1=http://…….., URI2=ldap://……. NON CRITICA

In particolare il CN del titolare, per interoperabilità con il certificato inserito a bordo della Carta d'Identità Elettronica (CIE), è composto dai seguenti sottocampi separati fra loro mediante i seguenti caratteri speciali:

CodiceFiscale/IdCarta.HashFileDatiPersonali

Il valore inserito nel campo "CodiceFiscale" è il codice fiscale del cittadino, il valore inserito in IdCarta è il serial number della smartcard nella quale sono inserite le chiavi ed il certificato, il valore inserito in HashFileDatiPersonali è il valore dell'hash del file dei dati personali del cittadino calcolato mediante l'algoritmo di hash SHA-1 (a 160 bits) e codificato in formato BASE64. Tutti i dati da inserire nel certificato del cittadino sono forniti alla CA dall'unità operativa di gestione delle carte.

25 La sicurezza del circuito della CNS

Il servizio CNS di IT Telecom prevede misure di sicurezza che coprono l'intero ciclo di vita delle carte, in coerenza con le indicazioni contenute nelle Linee Guida. Le fasi di lavorazioni sono tracciate su apposito registro che viene sottoscritto dai relativi responsabili e conservati in modo protetto per 10 anni a decorrere dalla data dell'ultima registrazione inserita, con modalità analoghe a quelle previste per la gestione del Registro dei Certificati.

Tutti i flussi informativi che vengono generati durante l'intero processo tra i diversi soggetti che vi partecipano (Ente Emettitore, Ente Certificatore, Produttore delle Carte) utilizzano canali sicuri che garantisce autenticità, integrità e riservatezza delle informazioni scambiate.

Tutte le fasi che compongono il processo di emissione delle CNS prevedono misure tecniche e organizzative tali da garantire la tutela dei dati personali (DL 196/2003), analogamente a quanto previsto per il servizio di certificazione della firma digitale.

Per quanto riguarda la sicurezza fisica degli impianti si rimanda a quanto descritto nella parte generale del presente Manuale Operativo.

Di seguito vengono descritte le misure di sicurezza specifiche previste per la fase di produzione delle carte e quella di generazione dei certificati.

25.1 Fase di produzione delle carte

Il trattamento delle smartcard nelle fasi di produzioni si attua con le stesse modalità previste per i dispositivi di firma dei titolari di certificati qualificati per la firma digitale.

In particolare, il Certificatore garantisce che :

- nel corso del processo di produzione, le carte sono protette da codici che impediscono al personale non autorizzato la modifica della struttura interna delle stesse. Tutti gli addetti che operano sulle carte in questa fase sono muniti di una smartcard di autenticazione ed è previsto un sistema di sicurezza che registra tutte le operazioni effettuate, garantendo integrità e non-ripudio di tali informazioni;

- le carte non in lavorazione sono conservate in locali che ne assicurano la sicurezza e, ogni volta che transitano su siti diversi, vengono accompagnate da una bolla di consegna che è verificata dal responsabile delle sicurezza della sede di arrivo.
- Il registro delle carte è compilato per ogni singolo movimento in entrata ed in uscita con l'indicazione di data e ora e, una volta completato, è firmato dal Responsabile della Sicurezza e dall'Incaricato della Produzione.
- è garantita la possibilità di verificare che il totale delle carte valide e quelle scartate corrisponde con il numero delle carte complessivamente previste.
- le carte che per qualsiasi motivo non sono considerate valide, vengono conservate negli stessi locali sicuri dove sono conservate le carte valide. Tali scarti vengono distrutti solo dopo l'approvazione di questa operazione da parte di un'apposita commissione, composta da rappresentanti appartenenti ai diversi ruoli coinvolti.

25.2 Fase di generazione dei certificati

La generazione dei certificati prevede l'utilizzo di un'apposita *workstation.* Il software presente sulla workstation genera le coppie di chiavi RSA relative all'autenticazione in modalità sicura e genera le credenziali per l'accesso al servizio, che vengono memorizzate in un archivio cifrato.

PARTE VI

Protezione dei Dati

In considerazione della grande importanza attribuita alla tematica del trattamento dei dati personali nell'ambito del Gruppo Telecom Italia, è operativo un sistema organizzativo e normativo interno per garantire che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni di legge vigenti e dei principi di correttezza e liceità dichiarati nel codice etico del Gruppo. Il complesso delle misure previste e messe in atto dal sistema implementato nel Gruppo Telecom Italia incorporano anche le misure minime previste dal **Codice per la protezione dei dati personali**

Tale sistema si caratterizza per alcune importanti elementi di base, fra i quali si ricordano i seguenti:

- i dipendenti che hanno ricevuto la nomina di incaricati ai sensi dell'art. 30 del DL 196/03, hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali.
- il trattamento dei dati personali avviene sotto la supervisione di responsabili del trattamento, anch'essi formalmente nominati, i quali hanno a loro volta ricevuto le necessarie istruzioni ed indicazioni operative.
- apposite funzioni aziendali hanno il compito di definire le policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate.
- il sistema di policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati.
- la tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali.
- le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

Nell'ambito delle policy di sicurezza aziendale sono state sviluppate soluzioni tecniche ed organizzative per la protezione dei dati trasmessi e conservati sulla rete e sui sistemi aziendali, fra cui rientrano:

- protezione dai virus con aggiornamento continuo;
- hardening dei sistemi utilizzati;
- software distribution per l'aggiornamento automatico delle patch di sicurezza sui sistemi aziendali;
- tool e metodologie di vulnerability assessment e risk analisys;
- protezione informatica dei punti di accesso alla rete aziendale;
- partizionamento e protezione delle reti interne;
- monitoraggio della rete e dei sistemi per la prevenzione ed il contrasto degli incidenti di sicurezza.

26 Modalità di Protezione dei Dati

Il presente capitolo del Manuale Operativo ha lo scopo di illustrare le procedure e le modalità operative adottate dal Certificatore per il trattamento dei dati personali, nello svolgimento della propria attività di certificazione.

I dati personali, relativi al richiedente la registrazione, al titolare di certificati, al terzo interessato e a chiunque acceda al servizio, sono trattati, conservati e protetti dal Certificatore conformemente a quanto previsto dal **Decreto legislativo n. 196 del 30 giugno 2003** "Codice in materia di protezione dei dati personali", pubblicato sul Supplemento ordinario n. 123 della G.U. n. 174 del 29 luglio 2003.

La terminologia utilizzata nel presente capitolo è conforme a quella adottata dal DL 196/03, e parzialmente difforme da quella utilizzata nel TUDA e dal DPCM 2004. In particolare:

a) per **Titolare**, si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza (ovvero il Certificatore);
b) per **Responsabile** si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;
c) per **Incaricato** si intende la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile;

d) per "**Interessato**", si intende la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (ovvero il richiedente la registrazione, il titolare di certificati, il terzo interessato o chiunque acceda al servizio).

In particolare, il Certificatore:

- nomina, se del caso, un **Responsabile del trattamento dei dati**, individuandolo all'interno dell'organizzazione aziendale e comunicandogli analiticamente e per iscritto i compiti che dovrà assolvere, ai sensi dell'Art. 29 del DL 196/03;
- individua e nomina i **funzionari Incaricati del trattamento dei dati** (ovvero gli Incaricati dell'Identificazione e quanti altri tratteranno i dati attinenti il servizio), che operano sotto la diretta autorità del Cliente (si veda il par. 12.1) o del Responsabile del Servizio, attenendosi alle istruzioni impartite, ai sensi dell'Art. 30 del DL 196/03;
- nomina eventuali **Responsabili esterni per il trattamento dei dati** specificando analiticamente i compiti per iscritto ed effettua, anche tramite verifiche periodiche, controlli sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni.

26.1 Definizione e identificazione di "Dati personali"

Ai sensi dell'Art. 1, comma 2, lett. b) del DL 196/03, per *dato personale* si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"; pertanto sono dati personali anche i codici identificativi forniti dal Certificatore, i puntatori e i PIN.

Dati personali potranno inoltre essere quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi - elettronici o cartacei - di registrazione, di richiesta di sospensione e di riabilitazione, di revoca, di cambio anagrafica e nei certificati, di cui ai relativi capitoli del presente Manuale Operativo. Al fine di garantirne un trattamento adeguato, le misure di sicurezza predisposte dal Certificatore e analiticamente descritte nel Piano per la Sicurezza, sono realizzate conformemente a quanto previsto dal DL 196/03.

26.2 Tutela e diritti degli interessati

In materia di trattamento dei dati personali il Certificatore garantisce la tutela degli interessati in ottemperanza al DL 196/03. In particolare:

- agli interessati sono fornite le necessarie informazioni ai sensi dell'Art. 13 (quali ad esempio il titolare, le modalità e finalità del trattamento, l'ambito di comunicazione e di diffusione, nonché i diritti di accesso ai suoi dati ai sensi dell'Art. 7);
- agli interessati viene richiesto, laddove necessario, il consenso scritto al trattamento dei propri dati personali.

26.3 Applicazione del Codice per la protezione dei dati personali

26.3.1 Adempimenti generali

Dal punto di vista generale il Certificatore:

- predispone, conserva e aggiorna, nell'ambito delle attività di certificazione, un *Registro degli Archivi Informatici e Cartacei* contenenti dati personali, incorporati nelle Banche Dati del Titolare e utilizzati nella gestione di tutte le fasi dell'attività di certificazione;
- definisce e aggiorna, con la supervisione del proprio Servizio Legale, i compiti dei suoi incaricati in relazione al trattamento degli archivi suddetti, in conformità con le misure minime di sicurezza previste dal DL 196/03 (Titolo V, capi I e II) e riportate nel Piano per la Sicurezza, nonché con le policy aziendali in materia di sicurezza e di tutela della riservatezza dei dati.

26.3.2 Adempimenti tecnici ed organizzativi

Dal punto di vista tecnico il Certificatore, (il Responsabile se nominato) tramite i suoi incaricati, adotta gli opportuni provvedimenti in relazione alla registrazione, elaborazione, conservazione, protezione dei dati personali, cancellazione/distruzione, secondo le modalità indicate qui di seguito.

26.3.2.1 Registrazione

- garantisce la conservazione dei dati tecnici relativi a struttura e formato degli archivi informatici e cartacei contenenti dati personali, nonché alla loro locazione fisica;
- supervisiona l'organizzazione e classificazione in maniera univoca degli archivi, nonché delle loro copie di sicurezza (backup) curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Certificatore. In proposito, si precisa che, a fronte di eventi che dovessero compromettere la capacità operativa del Certificatore presso la principale sede di attività, è definito un Piano Operativo che garantisce la disponibilità del registro dei certificati e le funzionalità di revoca e sospensione dei certificati in corso di validità.
- supervisiona l'organizzazione e classificazione in maniera univoca dei moduli di registrazione, accettazione, richiesta sospensione e riabilitazione, richiesta revoca, cambio anagrafica e qualsivoglia altro documento contenente dati personali, curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Certificatore.

26.3.2.2 Elaborazione

- controlla che l'elaborazione dei suddetti archivi e dei dati personali in essi contenuti sia effettuata esclusivamente per le finalità indicate nell'informativa resa ai sensi dell'Art. 13 del DL 196/03;
- verifica, in funzione del tipo di elaborazione, i formati di output e la destinazione finale dei dati al fine di garantirne la protezione, secondo quanto previsto nel seguito;
- rileva l'eventuale generazione di nuovi archivi nell'ambito delle fasi di elaborazione, supervisionando la loro classificazione.

26.3.2.3 Conservazione

- supervisiona la classificazione degli eventuali archivi – e dei dati in essi contenuti - soggetti a pura e semplice conservazione (archivi storici e/o di backup), riportando la durata della conservazione (inclusa data iniziale e finale), la natura del supporto e la sede di conservazione;
- si assicura che siano trattati come archivi di conservazione dei dati personali tutti gli archivi appartenenti a procedure temporaneamente bloccate o sospese;
- verifica che le procedure di conservazione di tutti i documenti utilizzati all'interno dell'attività di certificazione siano coerenti con la tutela dei dati personali.

26.3.2.4 Cancellazione/Distruzione

- verifica la registrazione - eventualmente in maniera automatizzata - della cancellazione/distruzione di singoli dati personali dagli archivi, riportando la tipologia dei dati, l'archivio interessato, la data di cancellazione/distruzione, nonché l'origine della cancellazione/distruzione (su richiesta dell'interessato, procedurale, accidentale, ecc.);
- verifica la registrazione della cancellazione/distruzione di archivi interi, secondo le modalità illustrate al punto precedente ed in conformità a quanto previsto dal DL 196/03, curando inoltre l'aggiornamento del *Registro degli Archivi Informatici e Cartacei*.

26.3.2.5 Protezione

- protegge la confidenzialità dei dati personali stabilendo le modalità di accesso agli archivi informatici e cartacei da parte dei soggetti abilitati appartenenti all'organizzazione del Certificatore. In particolare:
  - ✓ classifica i soggetti abilitati all'accesso in funzione delle loro mansioni. In particolare, si precisa che il Certificatore ha definito ed attua specifiche policy di gestione delle credenziali di autenticazione e per la costruzione e l'utilizzo delle password
  - ✓ registra le modalità di protezione dei dati, sia per quanto concerne la sicurezza logica degli archivi informatici (software di sicurezza, modalità di generazione del log delle elaborazioni, ecc.) che fisica (vigilanza dei locali, archiviazione documenti, gestione delle copie di sicurezza);
  - ✓ assicura la confidenzialità dei dati personali contenuti nei diversi formati di output delle fasi di elaborazione (cartacei, su terminale, ecc.) stabilendo le modalità operative necessarie, sia manuali che automatizzate;
  - ✓ supervisiona la circolazione interna delle informazioni contenute negli stampati (tabulati) o in altri supporti;

- ✓ assicura la distribuzione degli output su terminale in accordo con i profili utente designati dal responsabile della sicurezza;

- protegge l'integrità dei dati singolarmente considerati e degli archivi nel loro insieme, durante tutte le fasi di trattamento, stabilendo le modalità operative necessarie, sia manuali che automatizzate;
- garantisce la disponibilità dei dati, affinché il titolare possa adempiere alle richieste di consultazione/verifica da parte degli interessati previste dalla normativa vigente.

Ulteriori modalità di trattamento dei dati, oltre quella prevista dal DL 196/03, potranno essere previste a livello contrattuale tra il Certificatore e l'organizzazione, pubblica o privata che richieda il rilascio di più certificati, per conto di sottoscrittori a lei afferenti. In questo caso, tali accordi sono riportati all'interno del contratto di acquisto dei certificati da parte dell'organizzazione medesima.

26.4 Circostanze di rilascio di dati personali

Fermo restando il diritto dell'interessato di richiedere ed ottenere dal Certificatore informazioni relative ai propri dati personali, secondo quanto previsto dall'Art. 7 del DL 196/03, il Certificatore, nello svolgimento delle proprie attività di certificazione, può effettuare operazioni di comunicazione e diffusione dei dati personali .

In particolare:

- i dati personali possono essere comunicati all'Autorità Giudiziaria, in conformità con quanto previsto dalla normativa vigente;
- particolari accordi contrattuali possono prevedere destinatari e forme di comunicazione ulteriori rispetto a quanto previsto dal TUDA e dal DPCM 2004. Tali comunicazioni avverranno comunque nel rispetto della normativa vigente;
- ad esclusione di quanto previsto dal TUDA e dal DPCM 2004 in merito alla pubblicazione delle liste di revoca dei certificati, le motivazioni della revoca o sospensione dei certificati possono essere diffuse solo con il consenso esplicito dell'interessato.

PARTE VIII

Tavole di riferimento

Allo scopo di consentire la verifica della rispondenza del presente documento ai requisiti richiesti dalla vigente normativa, si riportano di seguito alcune tabella contenenti la corrispondenza fra la numerazione dei capitoli e paragrafi del presente Manuale Operativo e le disposizioni normative contenute nelle fonti seguenti:

- **TUDA**: Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, DPR 445/2000.
- **RT**: Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, DPCM 13/01/2004.

27 Tavola dei riferimenti al TUDA

Articolo	Comma	Numerazione del Manuale Operativo
10	3	19.1
23	1	19.3
23	2	10.4; 19.3
23	5	14.1
27 bis	1	10.7; 12.3.1; 14.1; (lett. d) 14.1.1
27 bis	2	14.1
27 bis	3	14.1; 10.2; 10.3; 10.4
28	3	15.2
29 bis	1	10.1; 10.4
29 bis	2	10.1; 10.2; 10.3; 15.1; 15.2; 16.1; 16.2; 18.2; 26
29 bis	3	8; 10.1; 10.2; 10.3; 12.3.2.1; 26
29 ter	1	10.8; 12.1.2; 14.1.1
29 sexies	1	13.1.2
29 sexies	2	19
29 sexies	4	19
29 septies	1	15.1; 15.3.1.1; 15.3.1.2
29 septies	3	16.2; 15.2

28 Tavola dei riferimenti al DPCM 2004

Articolo	Comma	Numerazione del Manuale Operativo
3	1	19; 20
3	2	19; 20;
3	3	19.1
4	1	13.2
4	2	10.4
4	3	10.4
4	4	8; 13; 22.3

4	5	8; 22.3
4	6	13.1.1
4	7	13
5	1	13
5	2	13
6	1	13.1.1
6	2	13.2
6	3	13.2; 10.4
6	4	10.1; 10.4; 13; 13.1.1; 19
6	5	10.4; 19
7	1	13; 10.1; 10.4
7	3	10.3
8	1	13.1.3
8	2	13.1.3
8	3	13.1.3
9	1	10.4; 13.2.1
9	2	13.2.1
9	3	13
9	4	13.2
9	6	13.2.1
9	7	13
10	1	10.1; 20
11	1	10.1.2
12	1	10.4; 14.3
14	1	14.2; 14.3
14	3	14; 18
14	4	14; 18
15	1	14.1
15	2	10.4
15	3	14
15	4	14
15	5	10.1; 14.2
16	1	15.1; 15.3.1; 15.3.2
17	1	15.2; 15.3.2
17	2	15.2
17	3	15.2
18	1	15.3.3.1
19	1	10.4; 15.3.1.1
19	2	10.4
19	3	15.1; 16.1
19	4	15.1; 16.1

20	1	15.3.1.2
20	2	15.3.3; 15.3.3.1
20	3	15.1
21	1	16.2
21	2	16.2
22	1	16.2.2.1
22	2	16.2.2
22	3	16.2
23	1	10.4
23	2	16.2
23	3	15.3
24	1	16
24	2	16.2.1
25	1	17.2
25	2	17.2
26	1	15.1; 15.4
26	2	15.4
26	3	15.2; 15.4
27	1	9; 18.2
27	2	14; 18
28	1	9
28	2	9
28	3	9
28	4	9
29	1	15.2; 16.2
29	2	15.3.2; 16.2
29	3	10.5
31	1	18
31	2	18
31	3	18.1; 21
31	4	18; 21
31	5	18.1; 21
31	6	18.1; 21
32	1	4
35	1	4
37	1	15.3.1
37	2	15.3.1
37	3	14.3.2
38	2	1
38	3	22.1 (lett. r); 19 (lett. t); 20 (lett. s)
39	2	21

39	3	21
40	2	10.1
42	1	19
43	1	13.1
44	1	22
44	2	22
45	1	22.2; 22.4
45	2	22.2
46	1	22.3
46	2	22.3
46	3	22.3
46	4	22.3
47	1	15.1
47	2	14.1
48	1	22.1; 22.2
48	2	22.2
49	1	22.5
49	2	22.5
49	3	22.5
49	4	4; 22.5
50	1	22.4.1
50	2	22.4.2
51	1	22
51	2	22.1
51	3	22.2
51	4	22.1
51	5	22.1
52		22; 22.4.2
53	1	13.2
53	2	13; 13.2
53	3	4