Certificatore InfoCert

Certificati di Sottoscrizione
Manuale Operativo

Codice documento: ICERT-INDI-MO

Questa pagina è lasciata
intenzionalmente bianca

Indice

Table of Contents

1. Introduzione al documento

Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	2.2	**Data Versione/Release**:	10/04/2010
Descrizione modifiche:	§4.1.6 §5.4.6		
Motivazioni:	Modifiche nell'operatività e nell'offerta adeguamento normativo		

Versione/Release n°:	2.1	**Data Versione/Release**:	03/12/2009
Descrizione modifiche:	§1.2 Riferimenti §2.2.1 sede legale §2.3 richiesta duplicato registrazione §§3.1.6, 5.4.1, 5.4.(2,4,5,6) Precisazione sugli obblighi del Richiedente, quando diverso dal Titolare §§4.1.1, 4.1.2.3, 4.1.5, 5.1, 5.2.5, 5.3, 5.4 Identificazione tramite firma digitale. §§7.3.6, 7.5 Conservazione ventennale marche temporali		
Motivazioni:	Modifiche nell'operatività e nell'offerta adeguamento normativo		

Versione/Release n°:	2.0	**Data Versione/Release**:	30/09/2009
Descrizione modifiche:	Precisazioni su revoche e sospensioni ampliamento del significato di dispositivo per la creazione della firma ai token USB e ai dispositivi HSM nuovo OID per nuova tipologia di firma Nuove modalità di riconoscimento tramite il circuito bancario		
Motivazioni:	Modifiche nell'operatività e nell'offerta		

Versione/Release n°:	1.4	**Data Versione/Release**:	12/09/2008
Descrizione modifiche:	§3.3.1, §5.2, §14		
Motivazioni:	Rilievi CNIPA		

Versione/Release n°:	1.3	**Data Versione/Release**:	05/05/2008
Descrizione modifiche:	§4.1.6, §12		
Motivazioni:	Estensione dei limiti di uso; Certificazione ISO9000		

Versione/Release n°:	1.2	**Data Versione/Release**:	05/11/07
Descrizione modifiche:	• Punto 11 §3.1.3		
Motivazioni:	Rilievo CNIPA. La versione 1.1 non è mai diventata operativa		

Versione/Release n°:	1.1	**Data Versione/Release**:	16/10/2007
Descrizione modifiche:	• Aggiornamento normativo • Indirizzo sede operativa e numero del call center • obblighi dei titolari (in linea con quanto previsto dalle linee guida CNIPA) • massimale assicurativo • caratteristiche del sistema di marcatura temporale		
Motivazioni:			

Versione/Release n°:	1.0	**Data Versione/Release**:	18/06/2007
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

1.1 Scopo e campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCert per l'emissione dei certificati per chiavi di sottoscrizione, nonché le procedure per la fornitura del servizio di validazione temporale se richiesto dagli utenti, in conformità con la vigente normativa in materia di firma digitale.
Il contenuto si basa sulle norme vigenti alla data di emissione e recepisce le raccomandazioni del documento *"Request for Comments: 2527 – Certificate Policy and certification practices framework"* © Internet Society 1999.

1.2 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come **CAD**) e successive modifiche e integrazioni

[2] *--- non utilizzato ---*

[3] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e sue modificazioni secondo DPR 137/2003 (nel seguito referenziato come **TU**)

[4] Deliberazione CNIPA 45/2009 (G.U. del 3-12-2009) – Regole per il riconoscimento e la verifica del documento informatico

[5] Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 (G.U. n. 129 del 6-6-2009)]. Referenziato nel seguito come **DPCM**

[6] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003)

[7] Circolare CNIPA n. 48 del 6 settembre 2005

[8] Legge 15 Marzo 1997, n. 59 (c.d. legge Bassanini)

[9] Legge 24 Dicembre 1993, n. 537

[10] Legge 23 Dicembre 1993, n. 547

[11] Legge 5 luglio 1991, n. 197 e successive modificazioni

[12] Decreto del Ministero del Tesoro del 19 dicembre 1991

[13] Ufficio Italiano Cambi: parere del 14 giugno 2001

[14] CIRCOLARE 19 giugno 2000 n. AIPA/CR/24

[15] D.Lgs. 21 novembre 2007, n. 231 "*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonchè della direttiva 2006/70/CE che ne reca misure di esecuzione*".

[16] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 12 ottobre 2007 (GU n. 13 del 16-1-2008) Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'articolo 13, comma 4, del decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003.

Riferimenti tecnici

[17] Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" - Aprile 2002

[18] RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[19] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

[20] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[21] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

1.3 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal **TU**, dal **CAD** e dal **DPCM** si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Accordi di Certificazione *[Cross-certification]*

La cross-certification si esercita tra Certification Authority che appartengono a domini diversi. In questo processo i Certificatori si certificano l'un l'altro. Condizione necessaria affinché possa avvenire la cross-certification è che essi accettino e condividano regole equivalenti nel Manuale Operativo.

Accreditamento facoltativo

Il riconoscimento del possesso, da parte del ***Certificatore*** che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Autocertificazione

E' la dichiarazione, rivolta al ***Certificatore***, effettuata personalmente dal soggetto che risulterà ***Titolare*** del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità, ai sensi dell'art. 46 del DPR 445/00 ed assunzione delle responsabilità stabilite per legge.

Autorità per la marcatura temporale *[Time-stamping authority]*

È il sistema software/hardware, gestito dal ***Certificatore***, che eroga il servizio di marcatura temporale.

Certificato, Certificato Digitale, Certificato X.509 *[Digital Certificate]*

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.

Nel certificato compaiono altre informazioni tra cui:

- il ***Certificatore*** che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificato Qualificato – cfr. CAD

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD

Certificatore Qualificato – cfr. CAD

Chiave Privata e Chiave Pubblica – cfr. CAD

Codice di emergenza
Codice preimbustato consegnato dall'Ufficio di Registrazione al ***Titolare*** per l'autenticazione della richiesta di sospensione di un certificato.

Dati per la creazione di una firma – cfr. DPCM

Dati per la verifica della firma – cfr. CAD

Dispositivo sicuro per la creazione della firma (SSCD)– cfr.CAD
Il dispositivo sicuro di firma utilizzato dal ***Titolare*** è un dispositivo crittografico rispondente a requisiti di sicurezza determinati dalla legge. Può essere una smart card, un token USB oppure un HSM.

Evidenza Informatica
Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

Firma digitale *[digital signature]* – cfr. CAD

Giornale di controllo
Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [5].

Lista dei Certificati Revocati o Sospesi *[Certificate Revocation List - CRL]*
E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea.
Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel **registro pubblico**.

Marca temporale *[Time Stamp Token]* – cfr. DPCM

Manuale Operativo – cfr. [5]
Il Manuale Operativo definisce le procedure che il ***Certificatore*** applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse da CNIPA e quelle della letteratura internazionale

Pubblico ufficiale
Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

RAO – Registration Authority Officer
Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un ***Titolare***, nonché ad attivare la procedura di certificazione per conto del ***Certificatore***.

Registro dei Certificati
Il Registro dei Certificati è un archivio che contiene tutti i certificati emessi dal ***Certificatore***.

Registro pubblico *[Directory]*
Il Registro pubblico è un archivio che contiene:
- tutti i certificati emessi dal ***Certificatore*** per i quali sia stata richiesta dal ***Titolare*** la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Regole tecniche

Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici [5].

Revoca o sospensione di un Certificato
È l'operazione con cui il ***Certificatore*** annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

Richiedente *[Subscriber]*
E' il soggetto che richiede all'Ente ***Certificatore*** il rilascio di certificati digitali. Se diverso dal ***Titolare***, l'identità del ***Richiedente*** è inserita nel campo Organization del certificato X.509.

Ruolo
Il termine Ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del ***Titolare*** del certificato, ovvero l'eventuale Potere di rappresentare persone fisiche o enti di diritto privato o pubblico, ovvero l'Appartenenza a detti enti nonché l'Esercizio di funzioni pubbliche.

Tempo Universale Coordinato *[Coordinated Universal Time]*
Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

Terzo Interessato – cfr. CAD
La persona fisica o giuridica che, ove previsto, presta il proprio consenso all'inserimento nel certificato di sottoscrizione di un Ruolo del ***Titolare*** o che autorizza o richiede l'inserimento nel certificato dell'indicazione dell'Organizzazione a cui il ***Titolare*** è collegato

Titolare *[Subject]*– cfr. CAD
La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al ***Titolare*** è attribuita la firma digitale generata con la chiave privata della coppia.

Uffici di Registrazione *[Registration Authority]*
Ente incaricato dal ***Certificatore*** a svolgere le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale nonché alla consegna del dispositivo sicuro di firma.

Utente *[Relying Party]*
Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma digitale basata su quel certificato.

1.4 Acronimi e abbreviazioni

ACBI – Associazione per il Corporate Banking Interbancario

CNIPA – Centro Nazionale per l'informatica nella Pubblica Amministrazione

CAD – Codice dell'amministrazione digitale
Ci si riferisce al D. Lgs n. 82/2005 e sue successive modificazioni, *"Codice dell'amministrazione digitale"*.

CRL – Certificate Revocation List

DN – Distinguished Name
Identificativo del ***Titolare*** di un certificato di chiave pubblica; tale codice è unico nell'ambito dei Titolari che abbiano un certificato emesso dal ***Certificatore***.

DPCM - Decreto del Presidente del Consiglio dei Ministri
Ci si riferisce al DPCM [5]

ETSI - European Telecommunications Standards Institute

HSM – Hardware Secure Module
E' un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

IETF - Internet Engineering Task Force

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

ISO - International Organization for Standardization
Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union
Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

IUT – Identificativo Univoco del Titolare
E' un codice associato al ***Titolare*** che lo identifica univocamente presso il ***Certificatore***; il ***Titolare*** ha codici diversi per ogni certificato in suo possesso.

LDAP – Lightweight Directory Access Protocol
Protocollo utilizzato per accedere al registro dei certificati.

OID – Object Identifier
E' costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

OTP – One Time Password
Meccanismo per l'autenticazione informatico basato sull'utilizzo non ripetibile di password. Può essere basato su dispositivi hardware o su procedure software.

PIN – Personal Identification Number
Codice associato ad un dispositivo sicuro di firma, utilizzato dal ***Titolare*** per accedere alle funzioni del dispositivo stesso.

PUK
Codice personalizzato utilizzato dal ***Titolare*** per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.

RRC
Acronimo di Revocation Request Code, nome assegnato in precedenza al codice di emergenza e saltuariamente ancora utilizzato.

SSCD – Secure Signature Creation Device
cfr. Dispositivo sicuro per la creazione della firma.

TSA – Time Stamping Authority
L'autorità di certificazione registrata presso il CNIPA che certifica le chiavi dei sistemi (cfr. TSU) che firmano le marche temporali (Time Stamp Token).

TST – Time-Stamp Token
Termine usato nella pubblicistica internazionale per la marca temporale.

TSU – Time Stamp Unit
Il componente fidato, le cui chiavi, certificate dalla TSA, firmano le marche temporali.

TU – Testo Unico
Ci si riferisce al DPR n. 445/2000 e sue successive modificazioni, *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*.

2. Generalità

Un certificato lega la chiave pubblica ad un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata: tale soggetto è il "***Titolare***" del certificato. Il certificato è usato da altri soggetti per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma digitale apposta o associata ad un documento.

Il certificato garantisce la corrispondenza tra la chiave pubblica ed il ***Titolare*** del certificato. Il grado d'affidabilità di quest'associazione è legato a diversi fattori: la modalità con cui il ***Certificatore*** ha emesso il certificato, le misure di sicurezza adottate, gli obblighi assunti dal ***Titolare*** per la protezione della propria chiave privata, le garanzie offerte dal ***Certificatore***.

Questo documento evidenzia le regole generali e le procedure seguite dal **Certificatore Accreditato** InfoCert (nel proseguo semplicemente indicato come il ***Certificatore***) per l'emissione e l'utilizzo di **Certificati Qualificati** (nel proseguo riferiti semplicemente come Certificati) di sottoscrizione.

La descrizione delle pratiche seguite dal ***Certificatore*** nell'emissione del certificato, delle misure di sicurezza adottate, degli obblighi, delle garanzie e delle responsabilità, ed in generale di tutto ciò che rende affidabile un certificato, viene riportato nel presente Manuale Operativo.
Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nei certificati, il ***Certificatore*** consente agli utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione e quindi del legame chiave - ***Titolare***.

2.1 Identificazione del documento

Questo documento è denominato "Certificatore InfoCert – Manuale Operativo" ed è caratterizzato dal codice documento: **ICERT-INDI-MO**.
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.
Al documento sono associati tre *object identifier,* referenziati nell'estensione CertificatePolicy dei certificati secondo l'utilizzo cui gli stessi sono destinati.
Il significato degli OID è il seguente:

L'*object identifier* (OID) **1.3.76.36.1.1.1** identifica:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
manuale-operativo-firma-digitale	1.3.76.36.1.1.1

L'*object identifier* (OID) **1.3.76.36.1.1.2** identifica:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Manuale-operativo-firma-automatica basata su HSM c/o InfoCert	1.3.76.36.1.1.2

L'*object identifier* (OID) **1.3.76.36.1.1.22** identifica:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Manuale-operativo-firma-applicata tramite HSM (**CAD** Art. 35 comma 3, [16])	1.3.76.36.1.1.22

Le clausole del documento che si applicano **esclusivamente** a ciascuna tipologia sono così prefissate:

1.3.76.36.1.1.1 → **OID1 -**
1.3.76.36.1.1.2 → **OID2 -**
1.3.76.36.1.1.22 → **OID3 -**

OID1/OID3 - I certificati con questo OID, possono riportare l'ulteriore OID **1.3.76.24.1.1.2**, che indica l'aderenza delle procedure InfoCert alle regole previste da ACBI e recepite dall'accordo quadro con AssoCertificatori.

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo 4.1.6. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del Manuale Operativo.

Questo documento è pubblicato in formato elettronico presso il sito Web del ***Certificatore*** all'indirizzo: http://www.firma.infocert.it/doc/manuali.htm

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCert S.p.A. è il **Certificatore Accreditato** (ai sensi dell'art. 29 del **CAD**) che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle Regole Tecniche [5] e secondo quanto prescritto dal **CAD**. In questo documento si usa il termine Certificatore Accreditato, o per brevità ***Certificatore***, per indicare InfoCert.
I dati completi dell'organizzazione che svolge la funzione di ***Certificatore*** sono i seguenti:

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Piazza Sallustio 9 00187 Roma**
Sede operativa	**Via G.B. Morgagni 30H 00161 Roma**
Rappresentante legale	**Dott. Daniele Vaccarino** In qualità di Presidente del Consiglio d'Amministrazione
Amministratore Delegato	
N° telefono	**06-442851**
N° fax	**06-44285255**
N° Iscrizione Registro Imprese	**Codice Fiscale 07945211006**
N° partita IVA	**07945211006**
Sito web	http://www.firma.infocert.it/

2.2.2 Uffici di Registrazione

Il ***Certificatore*** si avvale sul territorio di Uffici di Registrazione per svolgere principalmente le funzioni di:

- identificazione e registrazione del ***Titolare***,
- validazione della richiesta del certificato,
- distribuzione ed inizializzazione del dispositivo sicuro di firma,
- attivazione della procedura di certificazione della chiave pubblica,
- supporto al ***Titolare*** e al ***Certificatore*** nel rinnovo/revoca/sospensione dei certificati.

L'Ufficio di Registrazione, anche tramite suoi incaricati, svolge in sostanza tutte le attività di interfaccia tra il ***Certificatore*** ed il ***Richiedente*** e tra il ***Certificatore*** ed il ***Titolare***.
Gli Uffici di Registrazione sono attivati dal ***Certificatore*** a seguito di un adeguato addestramento del personale impiegato, che potrà svolgere le funzioni di identificazione, ed eventualmente registrazione, anche presso il ***Richiedente*** o presso il ***Titolare***.

Il ***Certificatore*** verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo Manuale.

2.2.3 Registro dei Certificati

Le liste di revoca e di sospensione dei certificati sono pubblicate in un **registro pubblico** che contiene anche i certificati dei titolari che ne hanno fatto espressa richiesta.
Il **registro dei certificati**, che contiene **tutti** i certificati emessi dal ***Certificatore***, **non** è pubblico.
Il ***Certificatore*** utilizza sistemi affidabili per la gestione del **registro pubblico** e 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.

2.2.4 Applicabilità

I certificati emessi dal ***Certificatore*** Accreditato InfoCert nelle modalità indicate dal presente manuale operativo sono **Certificati Qualificati** ai sensi dell'art. 28 del CAD.

L'utilizzo dei certificati di sottoscrizione (Certificati Qualificati) è il seguente:

- il certificato emesso dal ***Certificatore*** sarà usato per verificare la Firma Digitale del ***Titolare*** cui il certificato appartiene.
- Il ***Certificatore*** InfoCert mette a disposizione per la verifica delle firme il prodotto descritto al §6. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.
- in presenza di accordi di certificazione, il ***Certificatore*** riconosce la validità delle regole del ***Certificatore*** accreditato con cui stipula l'accordo e viceversa. Pertanto il certificato emesso per l'altro ***Certificatore*** sarà usato unicamente per verificare la firma di tale ***Certificatore*** sui certificati qualificati da questi emessi.

2.3 Contatto per utenti finali e comunicazioni

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.
Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile Certificazione Digitale
Corso Stati Uniti 14
35127 Padova
Telefono: 049 828 8111
Fax : 049 828 8406

Call Center Firma Digitale: 199.500.130
Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it

Il Titolare può richiedere copia della documentazione a lui relativa, compilando e inviando il modulo disponibile sul sito www.firma.infocert.it e seguendo la procedura ivi indicata.
La documentazione verrà inviata in formato elettronico all'indirizzo di email indicato nel modulo.

2.4 Rapporti con il CNIPA

Il presente Manuale Operativo, compilato dal ***Certificatore*** nel rispetto delle indicazioni legislative, è stato consegnato, in copia, al Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) che lo rende disponibile pubblicamente.

Allo scadere di un anno dalla precedente richiesta o comunicazione il ***Certificatore*** conferma al CNIPA per iscritto la permanenza dei requisiti per l'esercizio dell'attività di certificazione.
Al momento della richiesta d'iscrizione, il ***Certificatore*** fornisce al CNIPA i dati identificativi richiesti, che vengono sottoscritti, conservati e pubblicati dal CNIPA.

Almeno 90 giorni prima della scadenza del periodo di validità delle proprie chiavi di certificazione, il ***Certificatore*** avvierà la procedura di sostituzione.
Il ***Certificatore*** si attiene alle regole emanate dal CNIPA al fine dello scambio delle informazioni attraverso un sistema sicuro di comunicazione.

3. Regole Generali

In questo capitolo si descrivono le condizioni generali con cui il ***Certificatore*** eroga il servizio di certificazione descritto in questo manuale.

3.1 Obblighi e Responsabilità

3.1.1 Obblighi del Certificatore

Il ***Certificatore*** è tenuto a garantire che (cfr. artt. 30 e 32 del CAD):

1. siano soddisfatte tutte le regole tecniche specificate nel DPCM [5];
2. **OID1/OID3** siano soddisfatte le modalità di riconoscimento del ***Titolare*** ai sensi delle norme [11], [12], [13] e [15], con particolare riguardo all'identificazione fisica del ***Titolare***;
3. il Sistema Qualità sia conforme alle norme ISO9001;
4. la richiesta di certificazione sia autentica;
5. sia specificata nel certificato qualificato, su richiesta dell'istante, e con il consenso del ***Terzo Interessato***, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;
6. la chiave pubblica di cui si richiede la certificazione non sia già stata certificata, per un altro soggetto ***Titolare***, nell'ambito del proprio dominio. Per la verifica nel dominio degli altri certificatori accreditati, il ***Certificatore*** si impegna a stabilire accordi con gli altri certificatori presenti nell'Elenco CNIPA, in base alle attuali conoscenze tecnologiche, per l'attivazione di tali controlli;
7. sia rilasciato e reso pubblico, se esplicitamente richiesto dal ***Titolare***, il certificato qualificato secondo quanto stabilito all'art. 32, comma 3, lett. b) del **CAD**;
8. i Titolari siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi nonché riguardo agli obblighi da essi assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi sicuri di firma;
9. il proprio sistema di sicurezza dei dati sia rispondente alle misure minime di sicurezza per il trattamento dei dati personali, secondo il Decreto Legislativo 30 giugno 2003, n. 196 ;
10. il certificato sia revocato tempestivamente in caso di:
    - richiesta da parte del ***Titolare,***
    - richiesta da parte del ***Terzo Interessato***
    - richiesta da parte del ***Richiedente***
    - di compromissione della chiave privata
    - di provvedimento dell'autorità
    - d'acquisizione della conoscenza di cause limitative della capacità del ***Titolare***
    - di sospetti di abusi o falsificazioni;
11. sia certa l'associazione tra chiave pubblica e ***Titolare***;
12. il codice identificativo assegnato a ciascun ***Titolare*** sia univoco nell'ambito dei propri utenti;
13. **OID1 -** non si rende depositario di dati per la creazione della firma del ***Titolare***;
14. le proprie chiavi private siano accuratamente protette mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
15. siano conservate per almeno 20 (venti) anni dalla data di scadenza del certificato le informazioni ottenute in fase di registrazione, di richiesta di certificazione, di revoca e di rinnovo;
16. siano custoditi per 20 (venti) anni in forma accessibile i certificati delle proprie chiavi pubbliche di certificazione.
17. alla data del rilascio siano esatte e complete le informazioni necessarie alla verifica della firma contenute nel certificato e rispetto ai requisiti fissati per i certificati qualificati
18. **OID1 -** al momento del rilascio del certificato il ***Titolare*** detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato.
19. **OID2/OID3 -** i dati per la creazione della firma siano sotto il controllo esclusivo del ***Titolare***.

3.1.2 Obblighi dell'Ufficio di Registrazione

L'Ufficio di Registrazione è tenuto a garantire:

1. che il ***Titolare*** sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma;
2. che il ***Titolare*** sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. che il ***Titolare*** sia informato in merito agli accordi di certificazione stipulati con altri certificatori;
4. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196 e relativo allegato B ;
5. la verifica d'identità del ***Titolare*** del certificato, il controllo e la registrazione dei dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;
6. la custodia con la massima diligenza delle proprie chiavi private e dei dispositivi sicuri di firma che le contengono, ai fini di preservarne la riservatezza e l'integrità;
7. la comunicazione al ***Certificatore*** di tutti i dati e documenti acquisiti durante l'identificazione allo scopo di attivare la procedura di emissione del certificato;
8. la verifica e inoltro al ***Certificatore*** delle richieste di revoca, sospensione e rinnovo attivate dal ***Titolare*** presso l'Ufficio di Registrazione;
9. l'esecuzione, ove prevista a suo carico dal presente Manuale Operativo, della revoca o sospensione dei certificati.

L'Ufficio di Registrazione terrà direttamente i rapporti con il ***Richiedente*** e con i Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Manuale Operativo.

3.1.3 Obblighi dei Titolari

Il ***Titolare*** deve garantire:

1. la correttezza, veridicità e completezza delle informazioni fornite al soggetto che effettua l'identificazione, per la richiesta di certificato;
2. **OID1** - la protezione e la conservazione delle proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
3. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo e dalle vigenti leggi nazionali e internazionali;
4. l'utilizzo di software per l'apposizione della firma che, se diverso da quello indicato dal ***Certificatore***, assicuri l'utilizzo di algoritmi e formati di firma conformi alle norme in vigore;
5. la richiesta di revoca o di sospensione dei certificati in suo possesso nei casi previsti dal presente Manuale Operativo ai §§ 5.4.1 e 5.4.4;
6. **OID1** - la protezione della segretezza e conservazione del codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità del dispositivo sicuro di firma in luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente i dati per la creazione della firma (chiave privata);
7. la protezione della segretezza e conservazione del codice di emergenza per richiedere la sospensione del proprio certificato;
8. l'uso esclusivo del dispositivo sicuro per la generazione delle firme fornito dal ***Certificatore***;
9. **OID1** -l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e la custodia e l'utilizzo personale del dispositivo di firma;
10. di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato il certificato;
11. di non apporre firme elettroniche avvalendosi di chiavi private basate su un certificato emesso in base ad un certificato di certificazione che a lui sia noto essere stato revocato;
12. **OID2/OID3** - la protezione della segretezza e la conservazione del dispositivo e/o dei codici utilizzati per l'attivazione della procedura di firma .

3.1.4 Obblighi degli Utenti

L'utente che utilizza un certificato del quale non è il ***Titolare***, ha i seguenti obblighi:
1. conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del ***Certificatore***, riportati nel Manuale Operativo del ***Certificatore*** stesso;
2. verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta. Deve verificare con particolare attenzione il periodo di validità e che il certificato non risulti sospeso o revocato controllando le relative liste nel registro dei certificati;
3. Verificare il rispetto dei limiti d'uso eventualmente inseriti nel certificato ;
4. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.1.5 Obblighi del Terzo Interessato

Il ***Terzo Interessato***, che, **avendo presa visione del presente Manuale Operativo**, manifesta il proprio consenso all'inserimento nel certificato di un Ruolo oppure autorizza o richiede l'indicazione dell'Organizzazione a cui il ***Titolare*** è collegato, è tenuto a:

1. attenersi a quanto disposto dal presente Manuale Operativo;
2. provvedere tempestivamente all'inoltro, con le modalità descritte ai paragrafi 5.4.2 e 5.4.5, della richiesta di revoca o sospensione nei casi previsti ai paragrafi 5.4.1 e 5.4.4.

3.1.6 Obblighi del Richiedente

Il ***Richiedente*** che, **avendo presa visione del presente Manuale Operativo**, acquisisce i certificati qualificati e/o i dispositivi di firma è tenuto a:

3. attenersi a quanto disposto dal presente Manuale Operativo;
4. provvedere tempestivamente all'inoltro, con le modalità descritte ai paragrafi 5.4.2 e 5.4.5, della richiesta di revoca o sospensione nei casi previsti ai paragrafi 5.4.1 e 5.4.4.

3.2 Clausola risolutiva espressa ai sensi dell'art. 1456 c.c.

L'inadempimento da parte dell'Ufficio di Registrazione, del ***Richiedente***, del ***Titolare*** o del ***Terzo Interessato*** dei rispettivi obblighi descritti nei precedenti punti `3.1.2`, `3.1.3`, e `3.1.5` costituisce inadempimento essenziale ai sensi dell'art. 1455 c.c. e dà facoltà al ***Certificatore*** di risolvere il contratto eventualmente intercorso con tali soggetti.. La risoluzione opererà di diritto al semplice ricevimento di una comunicazione, inviata dal ***Certificatore*** tramite raccomandata A.R., contenente la contestazione dell'inadempienza e l'intendimento di avvalersi della risoluzione stessa.

3.3 Limitazioni e indennizzi

3.3.1 Limitazioni della garanzia e limitazioni degli indennizzi

Il ***Certificatore*** ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato trattato ed accettato dal CNIPA, che ha come massimali:
- 1.500.000 euro per singolo sinistro
- 1.500.000 euro per annualità.

Il ***Certificatore*** si assume le responsabilità previste dal CAD per i soggetti che svolgono funzione di ***Certificatore***.

3.4 Pubblicazione

3.4.1 Pubblicazione di informazioni relative al Certificatore

Il presente Manuale Operativo è reperibile:
- in formato elettronico presso il sito web del ***Certificatore*** (cfr. § 2.1)
- in formato cartaceo, richiedibile sia al ***Certificatore*** sia al proprio Ufficio di Registrazione.

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative al ***Certificatore*** previste dal **DPCM** sono pubblicate presso l'elenco CNIPA dei certificatori.

3.4.2 Pubblicazione dei certificati

I certificati emessi usualmente non sono pubblicati.
L'utente che voglia rendere pubblico il proprio certificato può farne richiesta inviando l'apposito modulo (disponibile sul sito www.firma.infocert.it), firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione. L'invio deve avvenire via e-mail indirizzata a **richiesta.pubblicazione@cert.legalmail.it** seguendo la procedura descritta sul sito stesso.

3.4.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: **ldap://ldap.infocert.it**
Tale accesso può essere effettuato tramite i software messi a disposizione dal ***Certificatore*** e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP.
Il ***Certificatore*** potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

3.5 Verifica di conformità

Con frequenza non superiore all'anno, il ***Certificatore*** esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

3.6 Tutela dei dati personali

Le informazioni relative al ***Titolare*** ed al ***Terzo Interessato*** di cui il ***Certificatore*** viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico {chiave pubblica, certificato (se richiesto dal ***Titolare***), date di revoca e di sospensione del certificato}.
In particolare i dati personali vengono trattati dal ***Certificatore*** in conformità con il Decreto Legislativo 30 giugno 2003, n. 196.

3.7 Tariffe

3.7.1 Rilascio, rinnovo, revoca e sospensione del certificato

Le tariffe sono rese disponibili sul sito www.firma.infocert.it.

3.7.2 Accesso al certificato e alle liste di revoca

L'accesso al **registro pubblico** (certificati pubblicati e lista dei certificati revocati o sospesi) è libero e gratuito.

4. Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per:
- l'identificazione del ***Titolare*** al momento della richiesta di rilascio del certificato qualificato di sottoscrizione;
- l'autenticazione del ***Titolare*** nel caso di rinnovo, revoca e sospensione del certificato qualificato di sottoscrizione;
- l'autenticazione dell'eventuale ***Terzo Interessato***, in caso di sua richiesta di revoca o sospensione del certificato qualificato del ***Titolare***.

4.1 Identificazione ai fini del primo rilascio

Il ***Certificatore*** deve verificare l'identità del ***Titolare*** prima di procedere al rilascio del certificato di sottoscrizione richiesto.
La procedura di identificazione comporta che il ***Titolare*** sia riconosciuto personalmente da uno dei soggetti di cui al §4.1.1, che ne verificherà l'identità attraverso il controllo della carta d'identità o di un documento ad essa equipollente (cfr. art. 35 comma 2 del **TU**) in corso di validità.

4.1.1 Soggetti abilitati ad effettuare l'identificazione

Ferma restando la responsabilità del ***Certificatore*** (§3.1.1), l'identità del soggetto ***Titolare*** viene accertata da:

Modalità 1
1. Il ***Certificatore***, anche tramite suoi Incaricati;
2. L'Ufficio di Registrazione, anche tramite suoi Incaricati;
3. Un Pubblico Ufficiale.

Modalità 2
Intermediari finanziari e altri soggetti esercenti attività finanziaria.

Modalità 3
Identificazione tramite firma digitale.

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 1

L'identificazione è effettuata da uno dei soggetti indicati al §4.1.1 (**Modalità 1**) ed è richiesta la **presenza fisica** del ***Titolare***.

1. Il soggetto che effettua l'identificazione verifica l'identità del ***Titolare*** tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato.

Al momento dell'identificazione viene fornito al ***Titolare*** un codice emergenza, che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra ***Certificatore*** e ***Titolare*** (cfr. art. 17 **DPCM**).

L'identificazione da parte dei Pubblici Ufficiali (cfr. Appendice B) può essere altresì effettuata in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 maggio 1991, n. 143 e successive modifiche ed integrazioni.

4.1.2.2 Riconoscimento effettuato secondo la modalità 2

Nella **modalità 2** il ***Certificatore*** si basa sul riconoscimento già effettuato da un Intermediario finanziario o da altro soggetto esercente attività finanziaria, che, ai sensi delle norme antiriciclaggio, è obbligato al riconoscimento certo dei propri clienti, con vincoli equivalenti a quelli previsti dalla normativa in tema di firma digitale [15[1]]. In questo caso, quindi, i dati identificativi del ***Titolare*** raccolti dall'intermediario all'atto del riconoscimento vengono utilizzati direttamente per l'emissione dei certificati, previa accettazione da parte del ***Titolare*** delle condizioni contrattuali per il rilascio del certificato e degli strumenti per l'apposizione della firma (siano essi SSCD o credenziali e strumenti per il controllo dei propri dati per la creazione della firma) nonché approvazione e conferma dei dati anagrafici registrati.

4.1.2.3 Riconoscimento effettuato secondo la modalità 3

Nella **modalità 3** il ***Certificatore*** si basa sul riconoscimento già effettuato da un altro ***Certificatore.*** Il ***Titolare*** è già in possesso di un dispositivo di firma con un certificato qualificato a bordo ancora in corso di validità. Il riconoscimento avviene in maniera analoga a quanto previsto dalla procedura di rinnovo (§4.2).
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.3 Modalità operative per la richiesta di rilascio del certificato di sottoscrizione

I passi principali a cui il ***Titolare*** deve attenersi per ottenere un certificato di sottoscrizione sono:

a) prendere visione del presente Manuale Operativo e dell'eventuale ulteriore documentazione informativa;
b) seguire le procedure di identificazione adottate dal ***Certificatore*** come descritte nel presente paragrafo;
c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
d) sottoscrivere la richiesta di registrazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio.

4.1.4 Informazioni che il Titolare deve fornire

Nella richiesta di registrazione sono contenute sia i dati relativi all'identità del cliente che le informazioni che consentono di gestire in maniera efficace il rapporto tra il ***Certificatore*** ed il ***Titolare***. Il modulo di richiesta **deve** essere sottoscritto dal ***Titolare***.

1 *Art 18 comma 1 lettera a) identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;*
Art. 19 comma 1 lettera a) l'identificazione e la verifica dell'identità del cliente e del titolare effettivo è svolta, in presenza del cliente, anche attraverso propri dipendenti o collaboratori, mediante un documento d'identità non scaduto, tra quelli di cui all'allegato tecnico, prima dell'instaurazione del rapporto continuativo o al momento in cui è conferito l'incarico di svolgere una prestazione professionale o dell'esecuzione dell'operazione.

Sono considerate **obbligatorie** le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale o analogo codice identificativo[2]
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso
- e-mail per l'invio delle comunicazioni dal ***Certificatore*** al ***Titolare***.

Opzionalmente il ***Titolare*** può fornire un altro nome, con il quale è comunemente conosciuto, che sarà inserito in un apposito campo denominato *commonName* (nome comune) del SubjectDN del certificato.
Il commonName, nel caso in cui non venisse fornito alcun ulteriore nome dal ***Titolare***, sarà valorizzato con nome e cognome del ***Titolare*** stesso.

4.1.5 Uso di pseudonimi

OID1 - E' facoltà del ***Titolare*** richiedere al ***Certificatore*** che il certificato riporti uno pseudonimo in luogo dei propri dati reali. Poiché il certificato è qualificato il ***Certificatore*** conserverà le informazioni relative alla reale identità dell'utente per venti (20) anni dopo la scadenza del certificato stesso.
L'uso dello pseudonimo NON è consentito per il riconoscimento nella modalità 3 (§4.1.2.3).

4.1.6 Limiti d'uso e limiti di valore

E' facoltà del ***Titolare*** richiedere al ***Certificatore*** l'inserimento nel certificato di limiti di valore che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. **I valori devono essere espressi come numeri interi positivi, senza indicazione di cifre decimali.**

Per quanto riguarda i limiti d'uso, allo stato attuale, InfoCert ha già predisposto questa indicazione per i certificati relativi a chiavi adoperate per l'apposizione di firme automatiche.

InfoCert rilascia anche certificati con la seguente limitazione d'uso:

Uso limitato alla firma di documenti informatici dell'Organizzazione indicata nel campo Organization del certificato per l'esercizio delle funzioni relative al ruolo ricoperto dal Titolare

Ferma restando la responsabilità del ***Certificatore*** di cui al **CAD** (art.30 comma 1 lettera a), è responsabilità dell'**Utente** verificare il rispetto dei limiti d'uso inseriti nel certificato.

La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dal ***Certificatore*** per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.

Oltre ai limiti suddetti, il ***Certificatore*** adotta i limiti d'uso pubblicati sul sito DigitPA che compariranno nel certificato come ulteriori Certificate Policy, così identificati:

1.3.76.36.1.1.23	I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
1.3.76.36.1.1.24.1	Il presente certificato è valido solo per firme apposte con procedura automatica. La presente dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati
1.3.76.36.1.1.24.2	The certificate may be used only for automatic procedure signature purposes.

2 Per i cittadini stranieri che non fossero in possesso del codice fiscale nè di alcun altro codice identificativo nazionale, deve essere presentato il passaporto, il cui identificativo sarà inserito nel certificato nello spazio predisposto per il codice fiscale nel formato PASSPORTXXXXX

1.3.76.36.1.1.25	L'utilizzo del certificato è limitato ai rapporti con *(indicare il soggetto)*. The certificate may be used only for relations with the *(declare the subject)*.

4.1.7 Inserimento del Ruolo e dell'Organizzazione nel certificato

Il ***Titolare*** può ottenere, direttamente, o con il consenso dell'eventuale ***Terzo Interessato*** , l'inserimento nel certificato di sottoscrizione di informazioni relative a *Funzioni, Titoli e/o Abilitazioni Professionali e Poteri di Rappresentanza*.

In questo caso, il ***Titolare***, oltre alla documentazione e alle informazioni identificative necessarie (cfr. §4.1.2, §4.1.4), dovrà produrre anche quella idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo, ove espressamente consentito dal presente Manuale Operativo, mediante Autocertificazione, ai sensi dell'art. 46 del D.P.R. 445/2000.

Come indicato nella Deliberazione CNIPA [4], nel caso in cui la richiesta di inserimento del ruolo nel certificato sia stata effettuata mediante la sola autocertificazione da parte del ***Titolare***, il certificato non riporterà informazioni inerenti l'organizzazione a cui potrebbe eventualmente essere legato il ruolo stesso.
Il ***Certificatore***, in tali ipotesi, non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, in merito all'inserimento nel certificato delle informazioni autocertificate dal ***Titolare***.

La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se essa ha richiesto (***Richiedente***) o autorizzato (***Terzo Interessato***) il rilascio del certificato al ***Titolare***, anche senza l'esplicita indicazione di un ruolo.

In tale ipotesi il ***Certificatore*** effettua un controllo sulla regolarità formale della documentazione presentata dal ***Titolare***.

La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni in possesso di Codice Fiscale.

Le informazioni inerenti al Ruolo che possono essere inserite nel certificato rientrano nelle seguenti categorie:

- Titoli e/o abilitazioni Professionali;
- Poteri di Rappresentanza di persone fisiche;
- Poteri di Rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi;
- Esercizio di Funzioni Pubbliche, Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi.

La tabella, esemplificativa e non esaustiva, dei Ruoli idonei all'inserimento nel certificato sarà disponibile in formato elettronico sul sito Web del ***Certificatore*** all'indirizzo:
http://www.firma.infocert.it/doc/manuali.htm

Il certificato con il Ruolo è conforme a quanto indicato nella Deliberazione CNIPA [4] e nel documento "Linee Guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei Titolari dei certificati elettronici" (OID=1.3.76.24.1.1.1) emesso da AssoCertificatori e disponibile sul sito http://www.assocertificatori.org.

4.1.7.1 Titoli e/o Abilitazioni Professionali

Nel caso in cui sia richiesta l'indicazione nel certificato di Abilitazioni Professionali per l'esercizio delle quali sia necessario ottenere preventivamente l'iscrizione all'Albo su verifica dell'Ordine

professionale competente alla tenuta e vigilanza dello stesso, il ***Titolare***, salvo diversa pattuizione tra il ***Certificatore*** e l'Ordine di appartenenza, dovrà fornire un certificato rilasciato dall'Ordine, o un'autocertificazione ai sensi dell'art. 46 del D.P.R. n. 445/2000, ed il consenso scritto da parte di quest'ultimo manifestato sull'apposito modulo fornito dal ***Certificatore***.
La documentazione da presentare ai sensi dei commi precedenti non dovrà essere anteriore di oltre 10 (dieci) giorni alla data della richiesta di registrazione.

Il ***Certificatore*** si riserva di subordinare l'inserimento nel certificato delle informazioni che rientrano in questa categoria alla stipulazione di appositi accordi con i singoli enti, cui compete la gestione e tenuta degli albi, elenchi e/o registri professionali, per la disciplina delle modalità di attestazione del Ruolo del ***Titolare*** e l'adempimento di quanto previsto a loro carico in qualità di ***Terzo Interessato***.

Per l'esercizio delle professioni per le quali sia richiesto l'iscrizione ad appositi albi non soggetti al controllo e verifica da parte di un apposito ente, il ***Titolare*** potrà attestare eventuali titoli mediante Autocertificazione, ai sensi dell'art. 46 D.P.R. 445/2000

4.1.7.2 Poteri di rappresentanza di persone fisiche

Nel caso in cui sia richiesta l'indicazione nel certificato di un Ruolo relativo alla *Rappresentanza di persona fisica,* il ***Titolare*** dovrà fornire, all'atto dell'identificazione, la copia autentica della delega o procura notarile sottoscritta dalla persona rappresentata e l'attestazione di consenso di quest'ultima all'inserimento del Ruolo nel certificato; nei casi previsti dalla legge, la prescritta documentazione potrà essere costituita da copia autentica del provvedimento emesso dall'autorità giudiziaria competente.

Il ***Titolare*** dovrà fornire altresì gli elementi di cui al paragrafo §4.1.4 relativi anche al rappresentato, escluse le informazioni relative alle modalità di comunicazione tra ***Certificatore*** e ***Titolare*** indicate nell'ultimo punto dell'elenco.

4.1.7.3 Poteri di Rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi

Nel caso in cui sia richiesta l'indicazione nel certificato di un Ruolo relativo alla *Rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi,* il ***Titolare*** dovrà presentare, congiuntamente alla richiesta di registrazione:

- L'Autocertificazione, ai sensi dell'art. 46 D.P.R. 445/2000, relativamente al Ruolo di cui si chiede l'inserimento nel certificato;
- una lettera ufficiale su carta intestata dell'ente di appartenenza, recante data e numero di protocollo, nella quale l'organizzazione segnala al ***Certificatore*** il consenso all'inserimento dello specifico Ruolo nel certificato.

Nei casi previsti dalla legge, la prescritta documentazione potrà essere costituita da copia autentica del provvedimento emesso dall'autorità giudiziaria o amministrativa competente.

I dati che il ***Titolare*** dovrà fornire sono i seguenti:

- nome e cognome,
- codice fiscale,
- numero di telefono presso l'organizzazione,
- l'indirizzo di posta elettronica presso l'organizzazione,
- il Ruolo da inserire nel certificato.

- La lettera dell'ente di appartenenza deve contenere una dichiarazione che **impegna** l'organizzazione a **comunicare tempestivamente** al ***Certificatore*** ogni variazione alle informazioni sopra elencate.

La lettera deve essere firmata dal rappresentante legale dell'organizzazione o da altra persona munita di apposita procura notarile o risultante da pubblici registri.

La lettera deve riportare, inoltre, chiaramente almeno le seguenti informazioni, salvo varianti dipendenti dal particolare tipo di organizzazione:

- denominazione dell'organizzazione (es. ragione sociale);
- indirizzo della sede legale dell'organizzazione;
- numero di partita IVA;
- numero di iscrizione al Registro Imprese,
- nome, numero di telefono e numero di fax del rappresentante legale,

La data di redazione della lettera deve essere non anteriore a 30 (trenta) giorni alla data della richiesta di registrazione del ***Titolare***.

4.1.7.4 Esercizio di Funzioni Pubbliche, Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi.

Il ***Certificatore*** si riserva di subordinare l'inserimento nel certificato di informazioni relative all'Esercizio di Funzioni Pubbliche, ovvero Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi, alla stipulazione di appositi accordi con gli enti di competenza; tali accordi, oltre a garantire l'adempimento di quanto previsto per il ***Terzo Interessato***, consentiranno di individuare il Ruolo del ***Titolare*** nel rispetto dell'organizzazione interna dell'ente pubblico di appartenenza.

4.2 Autenticazione per rinnovo delle chiavi e certificati

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (*validity*) con gli attributi "valido dal" (*not before*) e "valido fino al*" (not after).*

NOTA

le date indicate negli attributi suddetti sono espresse nel formato

anno-mese-giorno-ore-minuti-secondi-timezone
{AAAAMMGGHHMMSSZ}

nella rappresentazione UTCTime prevista dallo standard di riferimento [16]

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

OID1 - Il ***Titolare*** del certificato può, tuttavia, rinnovarlo, prima della sua scadenza, autenticandosi al ***Certificatore*** firmando digitalmente la richiesta di rinnovo con la chiave privata corrispondente alla chiave pubblica contenuta nel certificato da rinnovare.

OID2/OID3 - Il ***Titolare*** del certificato può, tuttavia, rinnovarlo, prima della sua scadenza, facendone richiesta all'Ufficio di Registrazione che ha rilasciato il certificato. Se il ***Titolare*** è in possesso di un altro SSCD e di un certificato qualificato può inoltrare direttamente alla CA la richiesta di rinnovo, firmata digitalmente, all'indirizzo email indicato al §2.3. La richiesta dovrà riportare il codice fiscale e lo IUT del certificato di cui viene richiesto il rinnovo.

Il ***Titolare***, qualora nel certificato da rinnovare siano presenti informazioni relative al Ruolo, dovrà dichiarare, mediante Autocertificazione ai sensi dell'art. 46 D.P.R. 445/2000, che le suddette informazioni non hanno subito variazioni dalla data del precedente rilascio, confermando la validità delle stesse al momento del rinnovo.

Il ***Certificatore***, nei casi di cui al comma precedente, provvederà a notificare l'avvenuto rinnovo all'eventuale ***Terzo Interessato*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***.

4.3 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire su richiesta del ***Titolare,*** del ***Terzo Interessato***, nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo, del ***Richiedente*** ovvero su iniziativa del ***Certificatore***.
Il ***Certificatore*** autentica chi fa richiesta di revoca e sospensione.

4.3.1 Richiesta da parte del Titolare

Se la richiesta viene effettuata per telefono o via Internet, il ***Titolare***, esclusivamente per la funzione di sospensione, si autentica fornendo il codice di emergenza, consegnato assieme al certificato che intende sospendere.
Se la richiesta viene fatta presso l'Ufficio di Registrazione, l'autenticazione del ***Titolare*** avviene con le modalità previste per l'identificazione.

4.3.2 Richiesta da parte del *Terzo Interessato*

Il ***Terzo Interessato*** che richiede la revoca o sospensione del certificato del ***Titolare***, si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal ***Certificatore*** e munendolo, qualora si tratti di un ente, di timbro o altra segnatura equivalente.
La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 5.4.2.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del ***Terzo Interessato*** in apposite convenzioni da stipulare con lo stesso.

4.3.3 Richiesta da parte del *Richiedente*

Il ***Richiedente*** che richiede la revoca o sospensione del certificato del ***Titolare***, si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal ***Certificatore*** e munendolo, qualora si tratti di un ente, di timbro o altra segnatura equivalente.
La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 5.4.2.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del ***Richiedente*** in apposite convenzioni da stipulare con lo stesso.

5. Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del ***Certificatore***.

La registrazione iniziale è effettuata presso il ***Certificatore*** oppure presso un Ufficio di Registrazione.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e, ove applicabile, la consegna del dispositivo sicuro di firma sono previste diverse modalità.

OID1 - La **prima** modalità (nel seguito **Caso A**) consente al ***Titolare*** di concludere la procedura di certificazione entrando in possesso dell'SSCD (smart card o token USB) e del certificato di sottoscrizione immediatamente dopo la registrazione: in questo caso il RAO avvierà in presenza del ***Titolare*** la procedura di generazione della coppia di chiavi e, effettuate le opportune verifiche, di emissione del certificato.

OID1 - La **seconda** modalità (nel seguito **Caso B**) prevede una separazione tra la fase di identificazione, effettuata in presenza del ***Titolare***, e quella di registrazione ed emissione del certificato, che viene effettuata successivamente dai RAO.

OID1 - In entrambi i casi l'SSCD (smart card o token USB) viene personalizzata a cura del ***Certificatore*** con il PIN consegnato al ***Titolare*** al momento dell'identificazione. Nel **Caso B** l'SSCD è consegnato al ***Titolare*** in un secondo momento.

OID2 - La **terza** modalità (nel seguito **Caso C**) si applica esclusivamente alle chiavi destinate ad essere utilizzate per la sottoscrizione automatica e generate all'interno di dispositivi HSM gestiti dal ***Certificatore***.

OID3 - La **quarta** modalità (nel seguito **Caso D**) si applica esclusivamente alle chiavi destinate ad essere utilizzate per la sottoscrizione tramite HSM ai sensi delle norme vigenti.

OID1 - La **quinta** modalità (nel seguito **Caso E**) si applica esclusivamente ai Titolari già in possesso di firma digitale.

Le modalità operative per la registrazione iniziale, il rilascio del certificato e la consegna dell'SSCD e/o delle credenziali per il controllo dei dati per la creazione della firma, nei casi di identificazione da parte di un Pubblico Ufficiale, anche se svolte all'estero, sono descritte separatamente nell'appendice B del presente Manuale Operativo.

5.2 Rilascio del certificato

5.2.1 OID1 - Caso A: Chiavi generate in presenza del Titolare

Questa procedura prevede la presenza del ***Titolare*** in possesso della carta a microprocessore presso un Ufficio di Registrazione o presso il ***Certificatore***.

1. Il RAO, contestualmente all'identificazione, registra il ***Titolare*** e attiva la procedura di rilascio di certificato.
2. La procedura automatica sblocca il dispositivo sicuro di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia e la predisposizione della la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della smartcard (PKCS#10). Nel caso in cui il dispositivo

sicuro di firma abbia un PIN differente da quello di default, la procedura richiede l'inserimento del PIN da parte del ***Titolare***.
3. Il RAO, utilizzando il proprio dispositivo, firma il PKCS#10 imbustandolo in un PKCS#7 e la invia al ***Certificatore***.
4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo sicuro di firma inserendo il PIN già consegnato al ***Titolare*** in fase di identificazione

5.2.2 OID1 - Caso B: Chiavi generate dal Certificatore

Questa procedura viene effettuata dai RAO, presso i locali del ***Certificatore*** o presso gli Uffici di Registrazione.

1. Il RAO seleziona i dati di registrazione di un ***Titolare*** e attiva la procedura di richiesta di certificato.
2. La procedura automatica sblocca il dispositivo sicuro di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia e la predisposizione della la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della smartcard (PKCS#10).
3. Il RAO, utilizzando il proprio dispositivo, firma il PKCS#10 imbustandolo in un PKCS#7 e la invia al ***Certificatore***.
4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo sicuro di firma inserendo il PIN già consegnato al ***Titolare*** in fase di identificazione

La segretezza del PIN personale durante le fasi di personalizzazione della smart card (dispositivo sicuro di firma) è garantita da adeguati sistemi di cifratura. Tale codice PIN, generato in modo casuale, è conservato in modo protetto all'interno dei sistemi del ***Certificatore***, e viene comunicato secondo procedure sicure (procedure automatiche con imbustamento in busta chiusa) al solo ***Titolare***.
La smart card così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.
Al primo utilizzo della smart card il ***Titolare*** è obbligato a cambiare tale PIN.

5.2.3 OID2 - Caso C: Chiavi generate in dispositivi HSM

OID2 - Questa procedura viene effettuata da personale del ***Certificatore*** presso i locali che ospitano l'HSM ed i server collegati. Il certificato emesso è inviato al ***Titolare***. Certificato e chiavi sono resi "non funzionali" fino a che il ***Titolare*** stesso non provveda a richiederne l'attivazione.

5.2.4 OID3 - Caso D: Chiavi generate in dispositivi HSM

OID3 - Questa procedura viene effettuata da personale specializzato del ***Certificatore*** o da quest'ultimo debitamente autorizzato, presso i locali che ospitano l'HSM ed i server collegati.

5.2.5 OID1 - Caso E: Titolare già in possesso di firma digitale

OID1 – Il ***Titolare*** si collega al sito del ***Certificatore*** e compila il form di registrazione, firmandolo digitalmente. La procedura genera quindi la nuova coppia di chiavi sul dispositivo del ***Titolare***

5.2.6 Generazione delle chiavi

Le chiavi asimmetriche sono generate all'interno del Dispositivo Sicuro per la Creazione della Firma (SSCD) utilizzando le funzionalità native offerte dai dispositivi stessi.
L'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è di 1024 bit.

5.2.7 Protezione delle chiavi private

OID1 - La chiave privata del ***Titolare*** è generata e memorizzata in un'area protetta della carta a microprocessore che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.

OID2/OID3 - La chiave privata del ***Titolare*** è generata e memorizzata in un'area protetta del dispositivo HSM che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione cancella la propria memoria, a protezione dei dati in essa contenuti.

5.3 Emissione del certificato

L'emissione del certificato viene effettuata in modo automatico dalle procedure del ***Certificatore*** secondo i seguenti passi:

1) viene verificata la correttezza della richiesta di certificato controllando che:
   - il ***Titolare*** sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - al ***Titolare*** sia stato assegnato un codice identificativo unico nell'ambito degli utenti del ***Certificatore*** (IUT);
   - la chiave pubblica che si intende certificare sia una chiave valida, della lunghezza prevista e non sia già stata certificata per un altro ***Titolare***;
   - **OID1 -** la richiesta sia autentica e il ***Titolare*** possieda la corrispondente chiave privata
   - la coppia di chiavi funzioni correttamente;
2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta
3) si procede alla generazione del certificato
4) viene attestato il momento di generazione del certificato utilizzando quale riferimento temporale la data fornita dal sistema della Certification Authority e tale registrazione viene riportata sul giornale di controllo.
5) il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati;
6) **OID1 -** il certificato viene memorizzato all'interno del dispositivo sicuro di firma del ***Titolare***;
   OID2 - il certificato viene memorizzato nei server del ***Certificatore*** ed inviato al ***Titolare***
   OID3 - il certificato viene memorizzato nei server del sistema di emissione
7) si distinguono i casi:

   - **OID1 -** (*Caso A*): il ***Titolare*** è già in possesso del dispositivo sicuro di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.
   - **OID1 -** (*Caso B*): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di Registrazione personalmente al ***Titolare***.
   - **OID2 -** *(Caso C)*: il ***Titolare*** è già in possesso del dispositivo per l'attivazione della firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.
   - **OID3 -** *(Caso D)*: il ***Titolare*** è già in possesso del dispositivo/credenziali per l'attivazione della firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.
   - **OID1 -** *(Caso E)*: il ***Titolare*** è già in possesso del dispositivo/credenziali per l'attivazione della firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.

8) I dati anagrafici e l'identificativo univoco del ***Titolare*** (IUT) sono comunicati, qualora sia impostato il campo Organization e, eventualmente, il certificato contenga informazioni sul Ruolo del ***Titolare*** medesimo, al ***Terzo Interessato*** o ***Richiedente*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***.

5.3.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni relative al ***Titolare*** ed indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme a quanto specificato nella Deliberazione CNIPA [4]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.
Il certificato contiene un'apposita estensione [Qualified Certificate Statements - esi4-qcStatement-1 (OID: 0.4.0.1862.1.1)] la quale indica che il certificato è qualificato.

5.3.2 Pubblicazione del certificato

Al buon esito della procedura di certificazione il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico. Il ***Titolare*** che volesse rendere pubblico il proprio certificato potrà richiederlo tramite la procedura descritta al §3.4.2.

5.3.3 Validità del certificato

Il periodo di validità del certificato è determinato sulla base:

- dello stato della tecnologia;
- dello stato dell'arte delle conoscenze crittografiche;
- dell'utilizzo previsto per il certificato stesso.

L'intervallo di validità del certificato è espresso al suo interno nella modalità indicata al paragrafo §4.2.

5.4 Revoca e sospensione di un certificato

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e rendono **non valide** le firme apposte successivamente al momento della pubblicazione della revoca o sospensione.
I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal ***Certificatore***, emessa e pubblicata nel registro dei certificati con periodicità prestabilita.
Il ***Certificatore*** può forzare un'emissione non programmata della CRL in circostanze particolari.
L'efficacia della revoca e della sospensione si ha dal momento di pubblicazione della lista, attestato dalla data apposta alla registrazione dell'evento nel Giornale di Controllo del ***Certificatore***.

5.4.1 Motivi per la revoca di un certificato

Il ***Certificatore*** esegue la revoca del certificato su propria iniziativa o per richiesta del ***Titolare,*** del ***Terzo Interessato*** o del ***Richiedente.***
Le condizioni per cui **DEVE** essere effettuata la richiesta di revoca sono le seguenti:

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
   - sia stato smarrito il dispositivo sicuro di firma che contiene la chiave;
   - sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN);
   - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
2. il ***Titolare*** non riesce più ad utilizzare il dispositivo sicuro di firma in suo possesso (es. guasto del dispositivo);
3. si verifica un cambiamento dei dati del ***Titolare*** presenti nel certificato, ivi compresi quelli relativi al Ruolo, tale da rendere detti dati non più corretti e/o veritieri;
4. termina il rapporto tra il ***Titolare*** e il ***Certificatore***;
5. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

Il ***Titolare*** ha facoltà di richiedere la revoca di un certificato per un **qualunque** motivo dallo stesso ritenuto valido ed in qualsiasi momento.

5.4.2 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del soggetto che la pone in essere. Sono previsti i seguenti casi:

Revoca su iniziativa del Titolare
Il ***Titolare*** deve richiedere la revoca tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la revoca al ***Certificatore***.

Chi richiede la revoca è tenuto a sottoscrivere la richiesta di revoca e consegnarla all'Ufficio di Registrazione o inviarla direttamente al ***Certificatore*** per lettera o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

Il ***Certificatore***, qualora nel certificato oggetto della richiesta di revoca siano presenti informazioni relative al Ruolo del ***Titolare***, provvederà a comunicare l'avvenuta revoca all'eventuale ***Terzo Interessato*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***

Il ***Certificatore***, qualora nel certificato oggetto della richiesta di revoca sia presente l'Organization del ***Richiedente***, provvederà a comunicare l'avvenuta revoca al ***Richiedente*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***

Revoca su iniziativa del Certificatore
Il ***Certificatore*** attiva una richiesta di revoca con la seguente modalità:
1. il ***Certificatore*** comunica al ***Titolare*** l'intenzione di revocare il certificato, fornendo il motivo della revoca, nonché la data e l'ora di decorrenza;
2. la procedura di revoca del certificato viene completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL) gestita dal ***Certificatore*** medesimo.

Il ***Certificatore***, qualora nel certificato revocato siano presenti informazioni relative al Ruolo del ***Titolare***, provvederà a comunicare l'avvenuta revoca all'eventuale ***Terzo Interessato*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***.

Il ***Certificatore***, qualora nel certificato oggetto della richiesta di revoca sia presente l'Organization del ***Richiedente***, provvederà a comunicare l'avvenuta revoca al ***Richiedente*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***

Revoca su iniziativa del Terzo Interessato
La richiesta di revoca su iniziativa del ***Terzo Interessato*** deve essere effettuata secondo la seguente modalità:
1. il ***Terzo Interessato*** richiede per iscritto al ***Certificatore*** la revoca del certificato compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato. Il ***Terzo Interessato*** è tenuto ad autenticarsi secondo quanto previsto al paragrafo 4.3.2;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare***, secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla revoca del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

Modalità aggiuntive per la richiesta di revoca da parte del ***Terzo Interessato*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

Revoca su iniziativa del Richiedente
La richiesta di revoca su iniziativa del ***Richiedente*** deve essere effettuata secondo la seguente modalità:

1. il ***Richiedente*** richiede per iscritto al ***Certificatore*** la revoca del certificato compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato. Il ***Richiedente*** è tenuto ad autenticarsi secondo quanto previsto al paragrafo 4.3.2;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare***, secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla revoca del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

Modalità aggiuntive per la richiesta di revoca da parte del ***Richiedente*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

5.4.3 Procedura per la revoca immediata

Nel caso di compromissione della chiave è necessario attivare la procedura di **revoca immediata**. Il ***Titolare*** è tenuto ad effettuare la richiesta di revoca specificando l'avvenuta o sospetta compromissione della chiave, dando luogo così alla revoca immediata.
Il processo di revoca segue i passi descritti nei casi precedenti con la particolarità che la pubblicazione della lista dei certificati revocati (CRL) avviene immediatamente (cfr. i paragrafi 5.4.7).

5.4.4 Motivi per la Sospensione di un certificato

Il ***Certificatore*** esegue la sospensione del certificato su propria iniziativa o per richiesta del ***Titolare,*** del ***Terzo Interessato*** o del ***Richiedente.***
La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:
1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il ***Titolare***, il ***Terzo Interessato*** o il ***Certificatore*** acquisiscano elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato specificandone la durata; alla scadenza di tale periodo, alla sospensione seguirà o una revoca definitiva oppure la ripresa di validità del certificato.

5.4.5 Procedura per la richiesta di Sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda del soggetto che la pone in essere.
La sospensione ha **sempre** una durata limitata nel tempo.
La sospensione termina alle ore 24:00:00 dell'ultimo giorno del periodo richiesto.

> **NOTA BENE:**
> il giorno di termine della sospensione **non può** essere successivo al giorno di scadenza del certificato.

Sono previsti i seguenti casi:

Sospensione su iniziativa del Titolare
Il ***Titolare*** deve richiedere la sospensione con una delle seguenti modalità:
1. utilizzando la funzione di sospensione disponibile nel sito Web del ***Certificatore***. Per effettuare la richiesta il ***Titolare*** **deve** comunicare:
    1. i propri dati identificativi,
    2. l'identificativo univoco a lui assegnato (IUT),
    3. la motivazione,
    4. la data di fine sospensione,

5. il codice di emergenza;

2. telefonando al Call Center del ***Certificatore*** e fornendo le informazioni di cui al punto precedente. In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una **sospensione immediata** del certificato per una durata di **10 (dieci) giorni solari** in attesa della richiesta scritta del ***Titolare***; qualora il ***Certificatore***, direttamente o tramite un Ufficio di Registrazione, non riceva la richiesta sottoscritta entro il termine indicato, il certificato verrà riattivato.
3. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione al ***Certificatore***.

Il ***Titolare*** è tenuto a sottoscrivere la richiesta di sospensione e consegnarla all'Ufficio di Registrazione o inviarla direttamente al ***Certificatore*** per lettera o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

Il ***Certificatore***, qualora nel certificato sospeso siano presenti informazioni relative al Ruolo provvederà a notificare la richiesta di sospensione all'eventuale ***Terzo Interessato*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***, specificando la data e l'ora a partire dalla quale il certificato risulta sospeso e la data di termine della sospensione.

Sospensione su iniziativa del Certificatore

Il ***Certificatore*** attiva una richiesta di sospensione con la seguente modalità:

1. il ***Certificatore***, salvo casi d'urgenza, comunica al ***Titolare*** preventivamente l'intenzione di sospendere il certificato, fornendo il motivo della sospensione, la data di decorrenza e la data di termine della sospensione. Queste ultime informazioni saranno in ogni caso comunicate al più presto al ***Titolare***.
2. La procedura di sospensione del certificato viene completata con l'inserimento nella lista di revoca e sospensione (CRL) gestita dal ***Certificatore*** medesimo.

Il ***Certificatore***, qualora nel certificato sospeso siano presenti informazioni relative al Ruolo, provvederà a notificare la richiesta di sospensione all'eventuale ***Terzo Interessato*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***, specificando la data e l'ora a partire dalla quale il certificato risulta sospeso e la data di termine della sospensione.

Sospensione su iniziativa del Terzo Interessato

La richiesta di sospensione su iniziativa del ***Terzo Interessato*** deve essere effettuata secondo la seguente modalità:

1. il ***Terzo Interessato*** richiede al ***Certificatore*** per iscritto la sospensione del certificato, compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato, la decorrenza e la data di termine della sospensione. Il ***Terzo Interessato*** è tenuto ad autenticarsi secondo quanto previsto al paragrafo 4.3.2;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare*** secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato inserendolo nella lista di revoca e sospensione (CRL).

Modalità aggiuntive per la richiesta di sospensione da parte del ***Terzo Interessato*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

Sospensione su iniziativa del Richiedente

La richiesta di sospensione su iniziativa del ***Richiedente*** deve essere effettuata secondo la seguente modalità:

1. il ***Richiedente*** richiede al ***Certificatore*** per iscritto la sospensione del certificato, compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato, la decorrenza e la data di termine della sospensione. Il ***Richiedente*** è tenuto ad autenticarsi secondo quanto previsto al paragrafo 4.3.2;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare*** secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato inserendolo nella lista di revoca e sospensione (CRL).

Modalità aggiuntive per la richiesta di sospensione da parte del ***Richiedente*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

5.4.6 Ripristino di validità di un Certificato sospeso

Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL).
La riattivazione avviene nell'arco delle 24 ore successive alla data di termine della sospensione.

Il certificato viene inoltre riattivato entro 10 giorni dalla richiesta qualora non venga inviata la richiesta documentazione scritta o quest'ultima non sia coerente con quanto comunicato via web o via Call Center

5.4.7 Pubblicazione e frequenza di emissione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dal ***Certificatore***, immessa e pubblicata nel **Registro pubblico**.
La CRL viene pubblicata in modo programmato almeno ogni giorno (emissione ordinaria) e nel caso vi siano revoche o sospensioni pendenti si effettua una pubblicazione aggiuntiva (emissione straordinaria).
L'effettiva frequenza della pubblicazione della CRL è desumibile dall'apposita 'estensione (*NextUpdate*) presente nella CRL stessa.
Il ***Certificatore*** può, in circostanze particolari, forzare un'emissione non programmata della CRL (emissione straordinaria immediata), ad esempio nel caso in cui la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata).
La CRL è emessa sempre integralmente. Il momento della pubblicazione della CRL viene attestata utilizzando quale riferimento temporale la data fornita dal sistema della Certification Authority e tale registrazione viene riportata sul giornale di controllo. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di revoca o sospensione.

Il ***Certificatore*** si riserva la possibilità di pubblicare separatamente altre CRL, sottoinsiemi della CRL più generale, allo scopo di alleggerire il carico di rete.
L'acquisizione e consultazione della CRL è a cura degli utenti.
La CRL da consultare per lo specifico certificato è indicata nel certificato stesso secondo le norme vigenti.

5.4.8 Tempistica

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di 24 ore.
In caso di revoca o sospensione immediata il tempo di attesa è al massimo di 1 ora.

5.5 Sostituzione delle chiavi e rinnovo del Certificato

La procedura di richiesta di un nuovo certificato, che prevede la generazione di una nuova coppia di chiavi, deve essere avviata da parte del ***Titolare*** **prima** della scadenza del certificato (Cfr. §4.2) già in suo possesso;
La procedura di rinnovo si applica esclusivamente a certificati emessi dal ***Certificatore*** InfoCert.
Oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere ad una nuova registrazione.
Il certificato scaduto resterà archiviato per la durata di 20 (venti) anni.
Le chiavi private di firma di cui sia scaduto il certificato della relativa chiave pubblica, non possono essere più utilizzate.

6. Strumenti e modalità per l'apposizione e la verifica della firma digitale

InfoCert mette a disposizione un prodotto (denominato "Dike") gratuitamente scaricabile dai Titolari dal sito www.firma.infocert.it per consentire:

- di firmare digitalmente documenti a tutti i titolari in possesso di una smart card rilasciata da InfoCert;
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Deliberazione CNIPA [4].
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Circolare AIPA 24/2000 [14].

Gli ambienti in cui Dike opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo web sopra indicato.

Le istruzioni per l'utilizzo del prodotto sono incluse nel prodotto stesso e consultabili tramite la funzione di help. Nel documento denominato "Manuale d'uso di Dike", facente parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.

Il prodotto Dike è in grado di firmare qualsiasi tipo di file. La possibilità di visualizzare il file dipende dalla disponibilità sulla stazione di lavoro dell'utente di un adeguato prodotto.

NOTA BENE: Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD. E' cura del ***Titolare*** assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.
In Allegato C sono riportate le modalità operative, in riferimento ad alcuni formati, per accertarsi che il documento non contenga macroistruzioni o codici eseguibili. Una nota particolare meritano i file con estensione HTM o HTML. Questi file sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Questi file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc...) i quali ne forniscono una forte connotazione dinamica. E' pertanto decisamente sconsigliato fare affidamento al contenuto mostrato tramite il Browser senza analizzarne attentamente l'effettivo contenuto.

7. Servizio di Marcatura Temporale e Riferimento Temporale del Certificatore

Su richiesta degli utenti l'Ente Certificatore InfoCert fornisce un servizio di validazione temporale di documenti informatici, siano essi firmati digitalmente ovvero non firmati.

In generale, il servizio di marcatura temporale consente di stabilire l'esistenza di un documento informatico **prima** di un certo istante temporale associando all'evidenza informatica una data e ora certe validandola temporalmente.
Un'evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale ad essa associata: la marca temporale è una struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora).
La marca temporale viene firmata ed emessa da un sistema centrale ed affidabile, basato su una specifica autorità di certificazione (*Time Stamping Authority* (TSA)) che certifica le chiavi di un sistema fidato (*Time Stamp Unit* (TSU)) al quale gli utenti indirizzano le loro richieste secondo necessità; chiunque abbia richiesto e conservato una marca temporale per un certo documento potrà, in seguito, dimostrare che tale documento effettivamente esisteva alla data/ora riportate nella marca firmata da quella catena di certificazione TSU/TSA.

In particolare, la validazione temporale di un **documento firmato digitalmente** consente di verificare e considerare valida la firma digitale apposta anche quando il certificato del sottoscrittore risulti scaduto o revocato, purché l'assegnazione della marca temporale al documento sia stata effettuata durante il periodo di validità del certificato medesimo.

7.1 Richiesta di emissione o di verifica di marca temporale

Il servizio di marcatura temporale prevede di indirizzare le richieste di emissione o verifica delle marche temporali di documenti informatici al server TSU tramite moduli software opportunamente predisposti.

La richiesta di emissione/verifica marca temporale può essere effettuata utilizzando il software di firma/verifica fornito da InfoCert, che consente di apporre la marca temporale a ***documenti firmati digitalmente*** e di eseguirne un'immediata verifica.
Una volta accettata e registrata la richiesta ed effettuati gli opportuni controlli di correttezza, il server ***TSU*** la elabora, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della verifica opportunamente predisposto per la visualizzazione.

Le modalità di utilizzo del servizio sono stabilite dall'Ente Certificatore InfoCert.

Le tipologie di richiesta previste dal servizio di marcatura temporale consistono in:

- ***emissione*** di marca temporale
- ***verifica*** di marca temporale.

Per la richiesta di ***emissione*** di marca temporale, l'utente seleziona il documento informatico da marcare dal proprio personal computer; l'opportuna procedura software ne calcola l'hash, che invia poi alla TSU per la marcatura; l'utente riceve in risposta un unico file in formato MIME contenente il documento originale e la marca temporale ad esso associata.

Non è prevista l'emissione di più marche temporali per la stessa evidenza informatica, sottoscritte da diverse TSU, ovvero con chiavi diverse certificate dalla stessa TSA.

Per la richiesta di ***verifica*** di marca temporale, l'utente deve fornire, come dati in ingresso il file in formato MIME, contenente la marca temporale e il documento informatico a cui la marca è associata. Può in alternativa fornire il documento originale e la marca corrispondente

nel formato "Time Stamp Response" oppure "Time Stamp Token". L'utente che riceve la marca temporale svolge, mediante le procedure opportunamente predisposte, i seguenti controlli:

a) verifica la firma della TSU, validando la catena di certificazione, usando la chiave pubblica corrispondente alla chiave privata utilizzata per la generazione della marca temporale
b) verifica che il valore dell'impronta contenuto nella marca temporale corrisponda allo stesso valore dell'impronta che è stata inviata alla TSU in fase di richiesta.

Il sistema, effettuate tutte le verifiche necessarie, visualizza le seguenti informazioni:

- data e ora di creazione della marca temporale
- numero seriale, identificativo della marca temporale
- identificativo dell'ente emittente la marca temporale.

Il verificarsi di situazioni di errore durante la richiesta di emissione o verifica di marcatura temporale viene esplicitamente segnalato all'utente.

7.2 Emissione o verifica di marca temporale

L'emissione della marca temporale viene effettuata in modo automatico da un sistema elettronico sicuro (server TSU), gestito dal ***Certificatore***, in grado di calcolare con precisione la data e ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato, generare la struttura di dati contenente le informazioni specificate nel successivo paragrafo 7.4.1, sottoscrivere digitalmente detta struttura di dati.
L'operazione avviene secondo le fasi seguenti:

- l'utente, mediante le procedure predisposte dal ***Certificatore***, invia la richiesta di marcatura temporale del documento informatico, eventualmente prendendone precedente visione, al server TSU
- La TSU, ricevuta la richiesta di marcatura temporale contenente l'impronta dell'evidenza informatica da sottoporre a validazione temporale calcolata secondo l'algoritmo di hash SHA1, provvede a generare la struttura di dati di cui al successivo paragrafo 7.4.1: detta struttura contiene, tra le varie informazioni, l'impronta medesima e la data/ora corrente ottenuta da una fonte esatta. Il server TSU appone la firma alla struttura dati generata, ottenendo la marca temporale. Terminata correttamente la procedura di generazione della marca temporale, quest'ultima viene inviata all'utente.

7.3 Gestione della coppia di chiavi asimmetriche della TSA

7.3.1 Generazione della chiave di marcatura temporale della TSA

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware conforme ai requisiti di sicurezza previsti dal DPCM [5]. Viene usato l'algoritmo asimmetrico **RSA** con chiavi di lunghezza non inferiore a **2048 bit**.

7.3.2 Generazione della chiave di marcatura temporale della TSU

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware conforme ai requisiti di sicurezza previsti dal DPCM [5]. Viene usato l'algoritmo asimmetrico **RSA** con chiavi di lunghezza non inferiore a **1024 bit**.

7.3.3 Protezione della chiave privata della TSA e delle TSU

I dispositivi per la generazione della coppia di chiavi asimmetriche della TSA e delle TSU possono essere attivati solo da operatori appositamente autorizzati che provvedono allo sblocco del dispositivo crittografico inserendo una coppia di smartcard accompagnate dall'apposito PIN.
Le chiavi private sono generate e memorizzate all'interno dei dispositivi crittografici in modo tale da impedirne l'esportazione.

7.3.4 Ciclo di vita della chiave di marcatura della TSU

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata al sistema che fornisce il servizio. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale (chiavi TSU) vengono sostituite dopo un mese di utilizzazione, indipendentemente dalla validità del certificato di chiave pubblica corrispondente.

La sostituzione mensile della chiave di marcatura temporale avviene senza revocare il corrispondente certificato di chiave pubblica.

Le chiavi della TSA sono soggette allo stesso ciclo di vita delle chiavi di certificazione.

7.3.5 Distribuzione della chiave pubblica per la verifica della marca temporale

È garantita l'integrità e l'autenticità della chiave pubblica del server TSU in quanto distribuita tramite emissione di un certificato di chiave pubblica **sottoscritto** dal ***Certificatore*** InfoCert S.p.A.

L'emissione del certificato per la verifica delle marche emesse viene effettuato in modo automatico dalle procedure del ***Certificatore*** secondo i seguenti passi:

- viene generata la richiesta di certificato da parte del personale autorizzato e inoltrata alla CA InfoCert dedicata alla certificazione di chiavi di marcatura temporale (TSA)
- si procede alla generazione del certificato
- il certificato viene pubblicato nel registro dei certificati e reso disponibile a tutti.

Il formato del certificato di marcatura temporale, contenente la chiave pubblica della TSU, è conforme a quanto specificato nella Deliberazione CNIPA [4]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.

Per la certificazione di chiavi di marcatura temporale TSU il ***Certificatore*** utilizza, secondo la vigente normativa, una coppia di chiavi (TSA) diversa da quella utilizzata per firmare certificati relativi alle usuali chiavi di sottoscrizione.

7.3.6 Validità della marca temporale

Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile.

Per le marche EMESSE dal 3 dicembre 2009 (incluso) la conservazione si estende per un periodo non inferiore a 20 (venti) anni.

Per le marche EMESSE prima del 3 dicembre 2009 la conservazione si estende per un periodo non inferiore a 5 (cinque) anni, salvo diverse pattuizioni contrattuali.

La marca temporale e' valida per l'intero periodo di conservazione a cura del fornitore del servizio.

7.4 Marca Temporale

7.4.1 Formato e contenuto della marca temporale

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche esposte in RFC 3161 *"Internet X.509 Public Key InfrastructureTime Stamp Protocol (TSP)"* -

PKIX Working Group IETF – Agosto 2001. Queste specifiche soddisfano i requisiti della legge italiana per quanto riguarda le funzionalità ritenute essenziali dal legislatore relativamente al servizio di marcatura temporale.

Ogni marca temporale emessa contiene tutte le informazioni richieste dalla normativa, ovvero:

- l'identificativo dell'emittente la marca temporale.
- il numero di serie della marca temporale.
- l'algoritmo di sottoscrizione della marca temporale. Nella fattispecie l'algoritmo utilizzato è l'RSA.
- l'identificativo del certificato relativo alla chiave pubblica della TSU.
- la data e l'ora di generazione della marca.
- l'identificativo dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale
- il valore dell'impronta dell'evidenza informatica.

7.4.2 Precisione del riferimento temporale

In fase di generazione di una marca temporale, il server della TSA ricava la data/ora dal clock del sistema, mantenuto allineato con l'ora esatta **UTC** (Tempo Universale Coordinato) grazie al segnale di sincronismo ottenuto da un ricevitore esterno di qualità del segnale emesso dalla rete dei satelliti GPS. Il segnale orario così ottenuto rispetta i margini di precisione richiesti dalla normativa vigente.

7.4.3 Tempistica

La generazione delle marche temporali garantisce che il tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, a meno di impedimenti nell'emissione della marca stessa, non sarà superiore al minuto primo.

7.5 Registrazione delle marche generate

Tutte le marche temporali emesse, assieme alle relative richieste sono conservate in un apposito archivio digitale non modificabile per cinque anni.

L'accesso ai dati, contenuti nei diversi archivi, è consentito solo agli operatori opportunamente abilitati.
L'utente può ottenere una copia della marca temporale facendone richiesta all'indirizzo di posta elettronica riportato al §2.3 fornendo i seguenti dati:

- l'utenza con cui è stata richiesta la marca temporale (*)
- data di erogazione (*)
- ora di erogazione (*)
- numero seriale della marca.

I dati contrassegnati con (*) sono **OBBLIGATORI**.

7.6 Sicurezza del sistema di validazione temporale

Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati tramite l'utilizzo di una serie di password e disponendo di un certo numero di smartcard.
Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione.

Un eventuale arresto del sistema può essere risolto solamente dagli operatori autorizzati.

Il sistema TSU dispone di uno specifico componente dedicato al monitoraggio delle seguenti condizioni:

1. tentativi di manomissione della sicurezza del sistema
2. perdita del segnale di sincronismo con la fonte esterna di tempo
3. degrado delle prestazioni in termini di tempo di risposta
4. disponibilità del supporto di archiviazione non riscrivibile

Al verificarsi di una o più delle suddette condizioni, viene valutata la gravità dell'evento, provvedendo all'arresto del servizio di marcatura temporale qualora non sussistano le necessarie misure di sicurezza.

8. Controllo del sistema di certificazione

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema di certificazione e dell'intera infrastruttura tecnica del ***Certificatore***.

8.1 Strumenti automatici per il controllo di sistema

Sono installati strumenti di controllo automatico che consentono al ***Certificatore*** di controllare il sistema valutando gli eventi e gli stati in cui il sistema stesso viene a trovarsi.

Il sistema è configurato in modo da intraprendere, in funzione dell'evoluzione dei suoi stati, delle azioni fra le seguenti tipologie:

- memorizzazione degli eventi;
- riconoscimento di eventi;
- risoluzione dei problemi;
- notificazione agli operatori.

8.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza del ***Certificatore*** sono soggette a controlli periodici legati sia alla verifiche ispettive per il conseguimento ed il successivo mantenimento della certificazione di qualità (ISO 9001) che a verifiche predisposte dalla funzione di auditing interno. Tali controlli mirano a verificare la corretta applicazione delle procedure previste e la loro effettiva funzionalità in relazione agli obiettivi prefissati.
Oltre alle attività di auditing di processi sono pianificate le analisi e i controlli da effettuare sulle registrazioni prodotte dalle applicazioni e dai sistemi durante il normale funzionamento. Tale attività ha lo scopo di controllare che tutti gli eventi verificatisi rientrino nella normale operatività e che non si verifichino eventi pregiudicanti la sicurezza. La registrazione e la conseguente imputabilità degli eventi verificatisi costituiscono inoltre una valida misura di sicurezza.

Gli eventi registrati e controllati (in modo automatico o manuale) sono:

- emissione dei certificati
- revoca dei certificati con la specificazione della data e dell'ora della pubblicazione della CRL;
- sospensione dei certificati con la specificazione della data e dell'ora della pubblicazione della CRL;
- inizio e fine sessione di lavoro sui sistemi preposti alla generazione dei certificati;
- personalizzazione dei dispositivi di firma;
- entrata ed uscita dai locali protetti;

Le registrazioni di questi eventi costituiscono il giornale di controllo.

9. Dati archiviati

Negli archivi gestiti dal ***Certificatore*** sono conservati e mantenuti i seguenti dati:

- certificati emessi, sospesi e revocati e relative marche temporali;
- dati di registrazione dei titolari delle chiavi;
- associazione tra codice identificativo del ***Titolare*** e dispositivo sicuro di firma;
- dati di sessione al sistema e ai servizi;
- dati inerenti al giornale di controllo;
- certificati delle chiavi di marcatura temporale.

L'accesso ai dati contenuti nei diversi archivi è consentito agli operatori opportunamente abilitati.
I dati archiviati sono conservati per 20 (venti) anni.

9.1 Procedure di salvataggio dei dati

Il salvataggio periodico dei dati relativi ai sistemi collegati in rete è effettuato giornalmente tramite un sistema di archiviazione automatizzato. Periodicamente copia dei supporti contenenti i dati del salvataggio viene archiviata in un armadio di sicurezza, il cui accesso è consentito unicamente all'operatore addetto che appartiene alla struttura del ***Certificatore***.
Periodicamente copia di tali supporti è inoltre trasportata in un luogo sicuro esterno alla sede del ***Certificatore***, in modo da averne la disponibilità anche in caso di eventi disastrosi.

A garanzia della possibilità di poter ripristinare il sistema completo a seguito di guasti, sono effettuati salvataggi di tutti gli altri dati e programmi necessari per l'erogazione del servizio. Le modalità e i tempi di archiviazione dei salvataggi sono gli stessi delle procedure di salvataggio dei dati.

10. Sostituzione delle chiavi del Certificatore

Il ***Certificatore*** effettua le procedure di sostituzione periodica della chiave privata di certificazione utilizzata per la firma dei certificati di sottoscrizione e di quella utilizzata per la firma dei certificati di marcatura temporale in maniera tale da consentire all'utente di poter utilizzare il certificato in suo possesso fino al momento del rinnovo.

11. Cessazione del servizio

Nel caso di cessazione dell'attività di certificazione, il ***Certificatore*** comunicherà questa intenzione al CNIPA con un anticipo di almeno 60 giorni, indicando, eventualmente, il ***Certificatore*** sostitutivo, il depositario del registro dei certificati e della relativa documentazione.

Con pari anticipo il ***Certificatore*** informa della cessazione della attività tutti i possessori di certificati da esso emessi. Nella comunicazione, nel caso in cui non sia indicato un ***Certificatore*** sostitutivo, sarà chiaramente specificato che tutti i certificati non ancora scaduti al momento della cessazione della attività del ***Certificatore*** saranno revocati.

12. Sistema di qualità

Tutti i processi operativi del ***Certificatore*** descritti in questo Manuale Operativo, come ogni altra attività del ***Certificatore***, sono conformi allo standard ISO9001.
InfoCert ha ottenuto la certificazione il 10 aprile 2008.

13. Disponibilità del servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (comprende i certificati e le CRL)	Dalle 0:00 alle 24:00 7 giorni su 7
Revoca e sospensione dei certificati	Dalle 0:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione, pubblicazione, rinnovo (*)	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi Dalle 9.00 alla 13.00 il sabato
Richiesta e/o verifica di marca temporale	24hx7gg (disponibilità minima 95%)

(*) L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono scegliere diversi orari di sportello. In ogni caso il ***Certificatore*** garantisce l'erogazione del proprio servizio negli orari sopra riportati.

14. Misure di Sicurezza

Il ***Certificatore*** ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di certificazione digitale.
Il sistema di sicurezza implementato è articolato su tre livelli:

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui il ***Certificatore*** gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Informazioni più dettagliate sul sistema di sicurezza adottato sono descritte in Appendice A.

14.1 Guasto al dispositivo sicuro di firma del Certificatore

In caso di guasto del dispositivo sicuro di firma del ***Certificatore*** si fa ricorso alla copia di riserva della chiave di certificazione, opportunamente salvata e custodita, e non vi è necessità di revocare il corrispondente certificato del ***Certificatore*** (cfr. §A.3).

14.2 Compromissione della chiave di certificazione

In caso di compromissione della segretezza della chiave privata di certificazione il ***Certificatore*** deve:

a) revocare il certificato della chiave di certificazione compromessa;
b) notificare la revoca al CNIPA entro 24 ore;
c) informare tutte i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata;
d) revocare tutti i certificati qualificati sottoscritti con la chiave compromessa;
e) nel caso di revoca del punto precedente saranno riemessi i certificati delle chiavi pubbliche dei titolari utilizzando una nuova chiave di certificazione.

14.3 Procedure di Gestione dei Disastri

Il ***Certificatore*** ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità o di disastro.

15. Amministrazione del Manuale Operativo

15.1 Procedure per l'aggiornamento

Il ***Certificatore*** si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.
Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.

Ogni modifica tecnica o procedurale a questo manuale operativo verrà prontamente comunicata agli Uffici di Registrazione.

Ogni variazione al manuale operativo sarà preventivamente comunicata al CNIPA che, per approvazione, provvederà a sottoscrivere e pubblicare sul proprio sito la nuova versione o release.

15.2 Regole per la pubblicazione e la notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del ***Certificatore*** (indirizzo: http://www.firma.infocert.it/doc/manuali.htm);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto dal CNIPA;
- in formato cartaceo può essere richiesto agli Uffici di Registrazione o al contatto per gli utenti finali (vedi §. 2.3).

15.3 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Responsabile dell'UO Certificazione Digitale e dal Responsabile Consulenza e Servizi Legali di InfoCert S.p.A..

15.4 Conformità

I contenuti del presente Manuale Operativo sono pienamente rispondenti alle regole tecniche descritte nel DCPM [5].

16. Appendice A: Descrizione delle misure di sicurezza

16.1 A.1 Sicurezza fisica

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a :

- Caratteristiche dell'edificio e della costruzione;
- Sistemi anti-intrusione attivi e passivi;
- Controllo degli accessi fisici;
- Alimentazione elettrica e condizionamento dell'aria;
- Protezione contro gli incendi;
- Protezione contro gli allagamenti;
- Modalità di archiviazione dei supporti magnetici;
- Siti di archiviazione dei supporti magnetici.

16.2 A.2 Sicurezza delle procedure

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate nella gestione dei certificati, è previsto di affidare la gestione operativa del sistema a persone diverse con compiti separati e ben definiti.
Il personale addetto alla progettazione ed erogazione del servizio di certificazione è dipendente dal ***Certificatore*** ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici e a caratteristiche di affidabilità e riservatezza.
Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa di certificazione, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati

16.3 A.3 Sicurezza logica

Generazione della coppia di chiavi
Il ***Certificatore*** per svolgere la sua attività ha bisogno di generare le seguenti chiavi:

- Chiave di certificazione per la firma dei certificati dei Titolari e del sistema di validazione temporale;
- Chiavi del sistema di validazione temporale per la marcatura temporale.

Le chiavi sono generate solamente da personale esplicitamente incaricato di tale funzione.
La generazione delle chiavi e della firma avviene all'interno di moduli crittografici dedicati.

La generazione delle chiavi di firma del ***Titolare*** avviene all'interno del dispositivo sicuro di firma (carta a microprocessore) rilasciato al ***Titolare*** stesso. L'attivazione del dispositivo, e quindi l'utilizzo delle chiavi in esso contenute, è subordinato alla digitazione del PIN.

Lunghezza delle chiavi
Le chiavi RSA usate dal ***Certificatore*** per firmare i certificati TSU sono di lunghezza: 2048 bit
Le chiavi RSA usate dal ***Certificatore*** per firmare i certificati dei Titolari sono di lunghezza: 2048 bit
Le chiavi per la firma delle marche temporali sono di lunghezza: 1024 bit.
Le chiavi di firma usate dal ***Titolare*** per apporre la firma digitale sono chiavi RSA ed hanno lunghezza di 1024 bit.

Protezione della chiave privata del Certificatore
La protezione delle chiavi private del ***Certificatore*** viene svolta dal modulo crittografico di generazione ed utilizzo della chiave stessa.
La chiave privata può essere generata solo con la presenza contemporanea di due operatori incaricati della generazione.

Le chiavi private del ***Certificatore*** vengono duplicate, al solo fine del loro ripristino in seguito alla rottura del dispositivo sicuro di firma, secondo una procedura controllata che prevede la suddivisione della chiave su più dispositivi.

Sicurezza dei sistemi del Certificatore
Per garantire la sicurezza dei dati e delle operazioni, tutto il software di sistema ed applicativo utilizzati per le funzioni del ***Certificatore*** realizza le seguenti funzioni di sicurezza:

- Identificazione e autenticazione degli utenti e dei processi che richiedono di operare nel sistema;
- Controllo accessi
- Imputabilità ed audit di ogni evento riguardante la sicurezza;
- Gestione delle risorse di memorizzazione volta ad impedire la possibilità di risalire alle informazioni in precedenza contenute o registrate da altri utenti;
- Autodiagnostica ed integrità dei dati e del software (controllo allineamento tra le copie operative e quelle di riferimento, controllo della configurazione del software, protezione dai virus).
- Configurazione hardware e software per garantire la continuità del servizio.

Livello di sicurezza dei sistemi operativi degli elaboratori
Il sistema operativo degli elaboratori utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, sono conformi alle specifiche previste dalla classe ITSEC F-C2/E2 oppure Common Criteria EAL4, equivalenti a quella C2 delle norme TCSEC.

Sicurezza della rete
Il ***Certificatore*** ha ideato per il servizio di certificazione un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi di firewalling e del protocollo SSL in modo da realizzare un canale sicuro tra gli Uffici di Registrazione ed il sistema di certificazione, nonché tra questo e gli amministratori/operatori. Il sistema è altresì supportato da specifici prodotti di sicurezza (anti intrusione di rete, monitoraggio, protezione da virus) e da tutte le relative procedure di gestione.

Controlli sul modulo di crittografia
Il modulo di crittografia utilizzato per la generazione delle chiavi e per la firma ha requisiti tali da assicurare:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo tale che non sia possibile l'intercettazione del valore della chiave privata utilizzata.

17. Appendice B: Modalità operative in caso di Identificazione da parte di Pubblico Ufficiale

17.1 B.1 Modalità operative in caso di Identificazione da parte di Pubblici Ufficiali in Italia

Alla data, la procedura di rilascio del certificato in caso di identificazione da parte di Pubblici Ufficiali in Italia non è ancora predisposta.

17.2 B.2 Modalità operative in caso di Identificazione da parte di Pubblici Ufficiali all'estero

Alla data, la procedura di rilascio del certificato in caso di identificazione da parte di Pubblici Ufficiali all'estero non è ancora predisposta.

18. Appendice C: Macroistruzioni

In questa appendice sono riportate le modalità operative per disabilitare l'esecuzione di macroistruzioni e codici eseguibili in alcune delle applicazioni di produttività individuale più comunemente utilizzate. Le applicazioni considerate sono in particolare: MS Word 2000, MS Excel 2000 e Acrobat Reader 6.0, tutte nelle relative versioni in lingua italiana.
Le estensioni dei file associate dal sistema operativo Windows a queste applicazioni sono comunemente le seguenti: .doc, .xls, .pdf. I documenti con queste estensioni sono, richiamando l'applicazione opportuna, direttamente visualizzate dall'applicazione di firma e verifica di cui al capitolo 6 di questo manuale operativo.
Si osservi che le indicazioni riportate in quest'appendice sono delle semplici linee guida per cui, per eventuali approfondimenti, è necessario fare riferimento ai manuali d'uso forniti a corredo delle singole applicazioni.

18.1 A.1 MS Word 2000 e MS Excel 2000

Macro
Le macro sono delle procedure automatizzate che permettono di fare diverse operazioni in sequenza. Esse possono essere eseguite all'atto dell'apertura di un documento e possono accedere a tutte le funzioni del sistema operativo.
Per verificare che sia attivata la protezione da Macro di MS Office 2000 si possono seguire i seguenti passi:

1. Fare clic sul menu **Strumenti**, scegliere **Macro**, quindi **Protezione**.
2. Selezionare il livello di protezione desiderato. Una protezione **Alta** consente l'apertura automatica (ovvero l'esecuzione) delle sole macro firmate digitalmente da fonti attendibili[3]. Le macro non firmate verranno disattivate automaticamente. Una protezione **Media** consente l'esecuzione automatica delle macro firmate digitalmente da fonti attendibili e di visualizzare la finestra di dialogo relativa alla protezione da virus macro che consente di disattivare le macro sospette.

Si noti che pur essendo disattivate le macro continuano ad essere presenti nel documento, pertanto sottoscrivendo il documento con firma digitale, si sottoscrivono anche le eventuali macro. Per tale ragione si consiglia di impostare il livello di protezione **Medio** in modo da avere evidenza della presenza delle stesse.

Per una panoramica completa del comportamento di MS Word 2000 e MS Excel 2000 in presenza di macro, consultare le Guide in linea dei prodotti alle voci "**Livelli di protezione in Word**" e "**Livelli di protezione in Excel**".

Codici automatici
I campi automatici o codici di campo di Word sono oggetti che possono essere inseriti all'interno di un documento. Essi contengono le istruzioni necessarie affinché Word possa convertirli in porzioni di testo recuperando le informazioni opportune in modo automatico dal contenuto del documento (indici,sommari, riferimenti), dalle sue proprietà (numero di pagine, autore del documento) o da quelle dell'elaboratore (data ed ora di sistema).
Per visualizzare/nascondere i codici di campo:

1. Fare clic sul menu **Strumenti**, scegliere **Opzioni**, quindi **Visualizza**.
2. Attivare la check box **Codici di campo** per visualizzare.
3. Selezionare dal sottostante menu **Ombreggiatura campo** : **Sempre**

3 L'elenco delle fonti attendibili può essere consultato ed aggiornato selezionando il menu **Strumenti**, **Macro**, quindi **Protezione** e **Fonti attendibili**.

MS Excel - Formule
Per visualizzare tutte le formule sul foglio di lavoro si sceglie **Strumenti** - **Opzioni** -**Visualizza** e si seleziona la check box **Formule**. Per nasconderle si esegue la stessa procedura e si deseleziona Formule.

18.2 A.2 Acrobat Reader (6.0 e 7.0)

Sebbene il formato PDF sia giustamente noto per la produzione di materiale di stampa, l'introduzione di un interprete Javascript in Acrobat e Acrobat Reader permette di realizzare documenti con contenuti ipertestuali e dinamici.
Per disattivare la possibilità di esecuzione di codice javascript in file pdf si possono seguire i seguenti passi:

1. Fare clic sul menu **Modifica**, scegliere **Preferenze...**
2. Nella listbox a sinistra della finestra **Preferenze** selezionare con un clic la voce **Javascript**
3. **Deselezionare la checkbox Abilita Javascript di Acrobat;**
4. da questo momento l'eventuale presenza di Javascript verrà segnalata da un messaggio.