"InfoCamere"
Società Consortile d'Informatica delle Camere di Commercio Italiane per azioni

Ente Certificatore InfoCamere

Certificati di Sottoscrizione

Manuale Operativo

Codice documento: ICCA-MO

Redatto da	**Fabio Uliano** Area Sistemi Sicurezza Informatica
Verificato da	**Alfredo Esposito** Area Sistemi Sicurezza Informatica
Verificato da	**Pio Barban** Area Sistemi Sicurezza Informatica
Approvato da	**Simone Nasoni** Direzione Prodotti e Servizi Applicativi
Approvato da	**Domenico Fantasia** Consulenza e Servizi Legali

Nome file: manualeoperativo_PRA_2.9_I.sxw

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento

Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	2.1a	**Data Versione/Release**:	10/07/2000
Descrizione modifiche:	Revisione del documento per la prima emissione in produzione – Modifica nome del sito web del Certificatore e riferimento circolare AIPA del 19 giugno 2000.		
Motivazioni:	Rilascio del servizio		

Versione/Release n°:	2.2	**Data Versione/Release**:	05/04/2001
Descrizione modifiche:	E' prevista una nuova modalità di distribuzione dei dispositivi di firma, con generazione delle chiavi da parte del Certificatore (§ 5.1, 5.1.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.3). Sono accettati come documenti di riconoscimento anche quelli equipollenti alla carta d'identità, secondo quanto stabilito dal Testo Unico (§ 4.1). Sono stati aggiornati i massimali dell'assicurazione (§ 3.2.1). I riferimenti al DPR 513/97 sono stati sostituiti con quelli al DPR 445/2000, Testo Unico delle Disposizioni Legislative e Regolamentari in materia di Documentazione Amministrativa. Sono stati modificati la durata del certificato e le relative tariffe (§ 3.7.1 e 5.3.3).		
Motivazioni:	Revisione procedura di riconoscimento e di rilascio dei dispositivi di firma, modifica della durata di validità dei certificati.		

Versione/Release n°:	2.3	**Data Versione/Release**:	7/9/2001
Descrizione modifiche:	E' stato aggiornato il nome del Rappresentante legale dell'organizzazione (§ 2.2.1). La sostituzione delle chiavi del certificatore è stata anticipata a due anni prima della scadenza della chiave di certificazione corrente; è stata modificata la durata dei certificati di cross-certification a due anni (§ 5.8).		
Motivazioni:	Aggiornamento dati riguardanti l'organizzazione InfoCamere S.C.p.A, modifica tempi di sostituzione delle chiavi del certificatore e durata dei certificati di cross-certification generati in fase di sostituzione medesima.		

Versione/Release n°:	2.4	**Data Versione/Release**:	27/9/2002
Descrizione modifiche:	Vengono indicate le procedure di validazione temporale di documenti elettronici e le modalità di conservazione delle marche temporali associate al relativo documento informatico.		
Motivazioni:	Fornitura del Servizio di validazione temporale		

Versione/Release n°:	2.5	**Data Versione/Release**:	16/06/2003
Descrizione modifiche:	Vengono indicati come soggetti abilitati ad effettuare l'identificazione del Richiedente il rilascio del certificato di sottoscrizione anche i pubblici ufficiali e descritte le procedure che il Richiedente deve seguire in fase d'identificazione qualora nel certificato venga richiesto l'inserimento dell'indicazione di funzioni, titoli e/o abilitazioni professionali o poteri di rappresentanza. Vengono, inoltre, indicati obblighi, responsabilità e facoltà in capo al Terzo Interessato.		
Motivazioni:	Certificazione di Funzioni, Titoli e/o Abilitazioni Professionali e Poteri di Rappresentanza nel certificato di sottoscrizione.		

Versione/Release n°:	2.6	**Data Versione/Release**:	08/07/2003
Descrizione modifiche:	Vengono integrate e/o modificate le definizioni che richiamano il T.U. secondo quanto indicato nel DPR 137/2003; in particolare il termine "certificato" è sostituito con il termine "Certificato Qualificato" e il termine Certificatore si riferisce ad un Certificatore Accreditato.		
Motivazioni:	Adeguamento del presente manuale operativo in seguito alla pubblicazione del DECRETO DEL PRESIDENTE DELLA REPUBBLICA 7 Aprile 2003, n° 137, Gazzetta Ufficiale, Serie Generale, n.138 del 17 Giugno 2003.		

Versione/Release n°:	2.7	**Data Versione/Release**:	10/11/2003
Descrizione modifiche:	E' stato sostituito il numero precedente per contattare il Call Center Firma Digitale con il nuovo numero stabilito.		
Motivazioni:	Modifica numero telefonico Call Center Firma Digitale.		

Versione/Release n°:	2.8	**Data Versione/Release**:	23/08/2004
Descrizione modifiche:	Paragrafo 2.2.1 aggiunti i riferimenti terza CA. Aggiornamento dei riferimenti normativi Adeguamento alle Nuove Regole Tecniche – DPCM 13 gennaio 2004		
Motivazioni:	Installazione nuova CA.		

Versione/Release n°:	2.9	**Data Versione/Release**:	13/12/2004
Descrizione modifiche:	Sono state aggiunte, delle informazioni su come accertarsi che il documento che si intende firmare digitalmente non contenga macroistruzioni e/o codice eseguibile (Cap. 6 e Appendice C: Macroistruzioni). E' stata modificato il paragrafo 5.3.3 relativo alla validità del certificato.		
Motivazioni:	Adeguamento alle Regole Tecniche 13/01/2004 Modificata la durata dei certificati da due a tre anni.		

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 InfoCamere 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 regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 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 del Presidente della Repubblica 7 Aprile 2003, n.137 (G.U. n.138 del 17 Giugno 2003)

[2] Decreto Legislativo 23 Gennaio 2002, n. 10 (G.U. n. 39 del 15 febbraio 2002)

[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] Circolare AIPA/CR/24 del 19 giugno 2000 (Linee Guida per l'interoperabilità dei Certificatori)

[5] Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004)

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

[7] Circolare AIPA/CR/22 del 26 Luglio 1999

[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

Riferimenti tecnici

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

[12] RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile

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

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

[15] 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 e dal DPCM 13 gennaio 2004 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. TU

Certificatore *[Certification Authority]* – cfr. TU

Certificatore Accreditato – cfr. TU

Certificatore Qualificato – cfr. TU

Chiave Privata e Chiave Pubblica – cfr. TU (Art. 22)

Dati per la creazione di una firma – cfr. TU

Dati per la verifica della firma – cfr. TU

Dispositivo sicuro per la creazione della firma – cfr.TU

Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da un supporto plastico (in genere una carta plastica delle dimensioni di una carta di credito) in cui è inserito un microprocessore rispondente a requisiti di sicurezza determinati dalla legge. E' chiamato anche **carta a microprocessore** o **smart card**.

Evidenza Informatica

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

Firma elettronica – cfr. TU

Firma elettronica avanzata – cfr. TU

Firma elettronica qualificata – cfr. TU

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

Giornale di controllo

Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dal Regolamento tecnico.

Lista dei Certificati Revocati o Sospesi *[Certificate Revocation List]*

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 lista CRL, che viene quindi pubblicata nel registro dei certificati.

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

Manuale Operativo – cfr. art. 38 DPCM

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 AIPA/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 *[Directory]*

Il Registro dei Certificati è un archivio che contiene:

- tutti i certificati validi emessi dal Certificatore;
- 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 (DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 gennaio 2004).

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

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. art. 29-bis TU , art. 20, 24 DPCM

La persona fisica o giuridica che, ove previsto, presta il proprio consenso all'inserimento nel certificato di sottoscrizione di un Ruolo del Richiedente.

Titolare *[Subject]*– cfr. art.1 TU

La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al Titolare e' 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

AIPA – Autorità per l'Informatica nella Pubblica Amministrazione (dal 30 luglio 2003 ha assunto la denominazione di **Centro Nazionale per l'informatica nella Pubblica Amministrazione - CNIPA**)

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 13 gennaio 2004.

DTS - Digital Time Stamping
Sistema per la marcatura temporale di certificati e documenti.

ETSI - European Telecommunications Standards Institute

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.

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 per ciascuna Smartcard, utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.

RRC – Revocation Request Code
Codice preimbustato consegnato dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di sospensione di un certificato.

TSA – Time Stamping Authority

TST – Time-Stamp token

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 d'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** InfoCamere (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 "Ente Certificatore InfoCamere – Manuale Operativo" ed è caratterizzato dal codice documento: **ICCA-MO**.
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

L'*object identifier* (OID) di questo documento è il seguente: 1.3.76.14.1.1.1
Tale OID identifica:

InfoCamere	1.3.76.14
certification-service-provider	1.3.76.14.1
certificate-policy	1.3.76.14.1.1
manuale-operativo-firma-digitale	1.3.76.14.1.1.1

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

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCamere S.C.p.A. è il **Certificatore Accreditato** (ai sensi dell'art. 11 DL 10/2002) che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle Regole Tecniche e secondo quanto prescritto dal Testo Unico. In questo documento si usa il termine Certificatore Accreditato, o per brevità Certificatore, per indicare InfoCamere.
I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Tabella 2

Denominazione Sociale	**InfoCamere - Società Consortile d'Informatica delle Camere di Commercio Italiane per azioni**
Sede legale	**Piazza Sallustio, 21 – 00187 Roma**
Rappresentante legale	**Dott. Giuseppe Pichetto** In qualità di Presidente del Consiglio d'Amministrazione
Direzione Generale	**Via G.B. Morgagni, 30H – 00161 Roma**
N° telefono	**06-442851**
N° fax	**06-44285255**
N° Iscrizione Registro Imprese	**Codice Fiscale 02313821007 (già Trib. di Roma 1 / 95)**
N° partita IVA	**02313821007**
Sito web	http://www.card.infocamere.it/
Nome X.500 prima Certification Authority	**CN=InfoCamere Firma Digitale,** **OU=Certification Service Provider,** **OU= Ente Certificatore del Sistema Camerale,** **O=InfoCamere SCpA,** **C=IT**
Nome X.500 seconda Certification Authority	**CN=InfoCamere Firma Digitale 2,** **OU=Certification Service Provider,** **OU= Ente Certificatore del Sistema Camerale,** **O=InfoCamere SCpA,** **C=IT**
Nome X.500 terza Certification Authority	**CN = InfoCamere Firma Qualificata** **OU = Certificatore Accreditato del Sistema Camerale** **SN = 02313821007** **O = InfoCamere SCpA** **C = IT**
Sede Operativa	**Corso Stati Uniti, 14 – 35127 Padova**

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 la certificazione.
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.
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 nel registro dei certificati. I certificati degli utenti saranno resi pubblici solo se esplicitamente richiesto dai titolari.

2.2.4 Applicabilità

I certificati emessi dal Certificatore Accreditato InfoCamere nelle modalità indicate dal presente manuale operativo sono **Certificati Qualificati** ai sensi dell'art.27 bis del T.U.

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 InfoCamere 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 avanzata di tale certificatore sui certificati qualificati da questi emessi.

2.3 Contatto per utenti finali e comunicazioni

InfoCamere 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:

InfoCamere S.C.p.A.
Responsabile Area Sistemi Sicurezza Informatica
Corso Stati Uniti 14
35127 Padova

Telefono: 049 828 8111
Fax : 049 828 8406

Call Center Firma Digitale: 199-763645
Web: http://www.card.infocamere.it
e-mail: firma.digitale@infocamere.it

2.4 Rapporti con il CNIPA (ex-AIPA)

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 (vedi §. 3.4.1), che vengono sottoscritti, conservati e pubblicati dal CNIPA.
Il Certificatore si impegna a comunicare al CNIPA la data di cessazione della propria attività di certificazione con un anticipo di almeno 60 giorni e ad informare i possessori dei certificati da questo emessi della revoca dei certificati al momento della cessazione dell'attività.
Almeno 90 giorni prima della scadenza del periodo di validità delle proprie chiavi di certificazione, il Certificatore avvierà la procedura di sostituzione e fornirà al CNIPA i certificati con firme incrociate previsti dalla procedura di rinnovo, attraverso il canale sicuro da essa predisposto.

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. art. 29-bis del TU):

1. siano soddisfatte le regole tecniche specificate nel DPCM ;
2. il Sistema Qualità sia conforme alle norme ISO9001;
3. la richiesta di certificazione sia autentica;
4. 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;
5. 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'Albo CNIPA, in base alle attuali conoscenze tecnologiche, per l'attivazione di tali controlli;
6. sia rilasciato e reso pubblico, se esplicitamente richiesto dal titolare, il certificato qualificato secondo quanto stabilito all'art. 29 bis, comma 2 lett. b) del T.U.;
7. i Richiedenti siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi nonché riguardo agli obblighi dei Titolari in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi sicuri di firma;
8. 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 ;
9. il certificato sia revocato tempestivamente in caso di richiesta da parte del Titolare o del Terzo Interessato, 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;
10. sia certa l'associazione tra chiave pubblica e Titolare;
11. il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
12. non si rende depositario di chiavi private;
13. le proprie chiavi private siano accuratamente protette mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
14. siano conservate per almeno 10 anni le informazioni ottenute in fase di registrazione, di richiesta di certificazione, di revoca e di rinnovo;
15. siano custoditi per 10 anni in forma accessibile i certificati delle proprie chiavi pubbliche di certificazione.

3.1.2 Obblighi dell'Ufficio di Registrazione

L'Ufficio di Registrazione è tenuto a garantire:

1. che il Richiedente 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 Richiedente sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. che il Richiedente 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 Richiedente il 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. 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. 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;
5. 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 la chiave;
6. la protezione della segretezza e conservazione del codice di autenticazione (RRC) per richiedere la sospensione del proprio certificato;
7. l'uso esclusivo del dispositivo sicuro per la generazione delle firme fornito dal certificatore;
8. l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 29-bis T.U.);

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

3.1.5 Obblighi del Terzo Interessato

Il Terzo Interessato, che, presa visione del presente Manuale Operativo, manifesta il proprio consenso all'inserimento nel certificato di un Ruolo, 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.

3.2 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 in nessun caso risponderà di eventi ad esso non imputabili ed in particolare di danni subiti dall'Ufficio di Registrazione, dal Titolare, dal Richiedente, dal Terzo Interessato, dagli Utenti o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.
Il Certificatore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

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:

- 1.549.369 euro per singolo sinistro
- 1.549.369 euro per annualità.

Il Certificatore si assume ogni responsabilità assegnata dal TU ai 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 all'indirizzo www.card.infocamere.it/doc/modulistica.htm) firmato digitalmente, via e-mail all'indirizzo **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 dei certificati accessibile con protocollo LDAP all'indirizzo: **ldap://ldap.infocamere.it** e **ldap://ldap2.infocamere.it** (per la terza Certification Authority elencata al § 2.2.1).
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 per la prima emissione, per il rinnovo, revoca e sospensione dei certificati qualificati sono le seguenti:

- Prima emissione: euro 7,75
- Rinnovo: euro 5,16
- Revoca e/o Sospensione: gratuita

Tali tariffe sono comunque funzione delle quantità trattate e soggette all'andamento del mercato.

Le tariffe indicate non comprendono il servizio di registrazione e il costo del dispositivo sicuro di firma (smart card).Accesso al certificato e alle liste di revoca

L'accesso al registro dei certificati pubblicati e alla lista dei certificati revocati o sospesi è libero e gratuito.

4. Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per:
- l'identificazione del Richiedente 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 con certezza l'identità del Richiedente prima di procedere al rilascio del certificato di sottoscrizione richiesto.
La procedura di identificazione comporta che il Richiedente 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

L'identità del soggetto Richiedente viene accertata da:
1. Il Certificatore, anche tramite suoi Incaricati;
2. L'Ufficio di Registrazione, anche tramite suoi Incaricati;
3. Un Pubblico Ufficiale.

4.1.2 Procedure per l'identificazione

L'identificazione è effettuata da uno dei soggetti indicati al § 4.1.1 ed è richiesta la presenza fisica del Richiedente.

Il soggetto che effettua l'identificazione verifica l'identità del Richiedente 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 Richiedente un codice segreto (RRC), che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e Titolare (cfr. art. 37 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.

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

I passi principali a cui il Richiedente 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 Richiedente deve fornire

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra il Certificatore ed il Richiedente/Titolare. Il modulo di richiesta deve essere sottoscritto dal Richiedente.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso
- Modalità di invio delle comunicazioni dal Certificatore al Titolare.

4.1.5 Inserimento del Ruolo nel certificato

Il Richiedente può ottenere, direttamente, e 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 Richiedente, 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.

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.card.infocamere.it/doc/manuali.htm

Il certificato con il Ruolo è conforme a quanto indicato 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.

4.1.5.1 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 Richiedente, 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 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 Richiedente 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 Richiedente potrà attestare eventuali titoli mediante Autocertificazione, ai sensi dell'art. 46 D.P.R. 445/2000

4.1.5.2 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 Richiedente 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 Richiedente 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.

4.1.5.3 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 Richiedente 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 Richiedente 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 Richiedente.

4.1.5.4 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 Richiedente 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).*
Si osservi che le date indicate negli attributi suddetti sono espresse nel seguente formato:
giorno-mese-anno-ore-minuti-secondi.

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

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.

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 all'eventuale Terzo Interessato l'avvenuto rinnovo.

4.3 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire su richiesta del Titolare o del Terzo Interessato, nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo , ovvero su iniziativa del Certificatore.
Il Certificatore autentica il richiedente la revoca e la 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 revoca segreto (RRC), 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.

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 la consegna del dispositivo sicuro di firma sono previste due diverse modalità.

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

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

In entrambi i casi la smart card viene personalizzata a cura del Certificatore con il PIN consegnato al Richiedente al momento dell'identificazione.
Nel **Caso B** la smart card personalizzata è consegnata al Richiedente (ora Titolare) in un secondo momento.

Le modalità operative per la registrazione iniziale, il rilascio del certificato e la consegna della smart card, 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 Caso A: Chiavi generate in presenza del Richiedente

Questa procedura prevede la presenza del Richiedente 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. 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 la richiesta di certificazione della chiave pubblica del Richiedente 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 Richiedente in fase di identificazione

5.2.2 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 Richiedente 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.
3. Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della smartcard 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 Richiedente 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.

5.2.3 Generazione delle chiavi

Le chiavi asimmetriche sono generate all'interno della carta a microprocessore utilizzando le funzionalità offerte dalla smart card stessa. La lunghezza delle chiavi è di 1024 bit.

5.2.4 Protezione delle chiavi private

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.

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 Richiedente sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - al Richiedente 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;
   - 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 emessa la marca temporale che attesta il momento della generazione
5) il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati;
6) il certificato viene memorizzato all'interno del dispositivo sicuro di firma del Titolare;
7) si distinguono i due casi:
   - (*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.
   - (*Caso B*): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di Registrazione personalmente al Titolare.
8) I dati anagrafici e l'identificativo univoco del Titolare (IUT) sono comunicati, qualora il certificato contenga informazioni sul Ruolo del Titolare medesimo, al Terzo Interessato, ove presente.

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 nelle Linee Guida per l'Interoperabilità dei Certificatori ; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.

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. L'utente 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 si estende fino a tre anni a partire dalla data d'emissione.
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 con marca temporale.

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 o del Terzo Interessato.
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.

5.4.2 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del richiedente. 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.

Il richiedente 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 revocato siano presenti informazioni relative al Ruolo del Titolare, provvederà a comunicare l'avvenuta revoca all'eventuale Terzo Interessato

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.

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.

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 su richiesta del Titolare o del Terzo Interessato. 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 richiedente. 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 i propri dati identificativi, l'identificativo univoco a lui assegnato (IUT), la motivazione e il periodo di durata della sospensione, il codice di revoca del certificato (RRC);
2. telefonando al Call Center del Certificatore e fornendo le informazioni di cui al punto precedente. In assenza del codice RRC 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 in attesa della richiesta scritta del Titolare;
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.
Qualora il Certificatore, direttamente o tramite un Ufficio di Registrazione, non riceva la richiesta sottoscritta entro 10 giorni solari dalla richiesta di sospensione, il certificato verrà riattivato.

Il Certificatore, qualora nel certificato sospeso siano presenti informazioni relative al Ruolo provvederà a notificare la richiesta di sospensione all'eventuale Terzo Interessato, specificando la data e l'ora a partire dalla quale il certificato risulta sospeso e la durata.

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 durata della sospensione. Quest'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, specificando la data e l'ora a partire dalla quale il certificato risulta sospeso e la durata.

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 durata 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.

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).

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 dei certificati.
La CRL viene pubblicata in modo programmato ogni giorno (emissione ordinaria) e nel caso vi siano revoche o sospensioni pendenti si effettua una pubblicazione aggiuntiva (emissione straordinaria).
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 e il momento della pubblicazione è asseverato mediante l'apposizione di una marca temporale. 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 utilizzatori.
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 2 ore.

5.5 Sostituzione delle chiavi e rinnovo del Certificato

Il certificato ha al massimo validità di tre anni dalla data di emissione. 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)

Il Titolare che intende rinnovare il suo certificato digitale deve richiedere l'emissione di un nuovo certificato prima della scadenza di quello in suo possesso.
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 10 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

InfoCamere mette a disposizione un prodotto (denominato "Dike") gratuitamente scaricabile dai Titolari dal sito www.card.infocamere.it per consentire:

- di firmare digitalmente documenti a tutti i titolari in possesso di una smart card rilasciata da InfoCamere;
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Circolare AIPA/CR/24 – 2000

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

http://www.card.infocamere.it/software/software_home.htm

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 ma permette di visualizzare solo quelli con le seguenti estensioni:

DOC (corrispondente al prodotto Microsoft Word)
XLS (corrispondente al prodotto Microsoft Excel)
PDF (corrispondente al prodotto Adobe Acrobat)
TIF
RTF
TXT
HTM/HTML

Alcuni di questi 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 10, comma 3 del Testo Unico. 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 InfoCamere fornisce un servizio di validazione temporale di documenti informatici, siano essi firmati digitalmente ovvero non firmati.
La marcatura temporale è, invece sempre applicata a certificati e liste di revoca e sospensione come riferimento temporale richiesto dalla normativa, in modo tale da attestarne il momento della pubblicazione.

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, detto *Time Stamping Authority* (TSA), 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 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 di TSA tramite moduli software opportunamente predisposti.

La richiesta di emissione/verifica marca temporale può essere effettuata utilizzando il software di firma/verifica fornito da InfoCamere, 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 di *Time Stamping Authority* la elabora, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della verifica opportunamente predisposto per la visualizzazione.

L'utente può, inoltre, effettuare la richiesta via Web: in questo caso potranno essere validati documenti informatici generici. Le modalità di utilizzo del servizio sono stabilite dall'Ente Certificatore InfoCamere.

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 TSA 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 con chiavi diverse da parte della medesima 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". L'utente che riceve la marca temporale svolge, mediante le procedure opportunamente predisposte, i seguenti controlli:

a) verifica la firma della TSA, 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 TSA 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 di TSA), 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 richiedente, mediante le procedure predisposte dal Certificatore, invia la richiesta di marcatura temporale del documento informatico, eventualmente prendendone precedente visione, al server di TSA
- La TSA, 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 di TSA 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 13 gennaio 2004. Viene usato l'algoritmo asimmetrico **RSA** con chiavi di lunghezza non inferiore a **1024 bit**.

7.3.2 Protezione della chiave privata della TSA

Il dispositivo per la generazione della coppia di chiavi asimmetriche della TSA può essere attivato solo da operatori appositamente autorizzati che provvedono allo sblocco del dispositivo crittografico inserendo una coppia di smartcard accompagnate dall'apposito PIN.

La chiave privata della TSA è generata e memorizzata all'interno del dispositivo crittografico in modo tale da impedirne l'esportazione.

7.3.3 Ciclo di vita della chiave di marcatura della TSA

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 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.

7.3.4 Distribuzione della chiave pubblica per la verifica della marca temporale

È garantita l'integrità e l'autenticità della chiave pubblica del server di TSA in quanto distribuita tramite emissione di un certificato di chiave pubblica **sottoscritto** dal Certificatore Infocamere S.C.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 InfoCamere dedicata alla certificazione di chiavi di marcatura temporale
- 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 TSA, è conforme a quanto specificato nelle Linee Guida per l'Interoperabilità dei Certificatori; 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 il Certificatore utilizza, secondo la vigente normativa, una coppia di chiavi diversa da quella utilizzata per firmare certificati relativi alle usuali chiavi di sottoscrizione.

7.3.5 Validità della marca temporale

Il periodo di validità del certificato di marcatura temporale si estende per quattro anni a partire dalla data di emissione. Una marca temporale ha validità fino alla scadenza del suddetto certificato: il periodo di validità può essere ulteriormente esteso associando, prima della scadenza del corrispondente certificato, una nuova marca all'intera evidenza informatica costituita dal documento originale marcato e precedente marca temporale.

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 TSA.
- 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: il server di marcatura temporale ricava il tempo da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettronico Nazionale (IEN) "Galileo Ferraris". Il ricevitore utilizzato è stato preventivamente tarato e certificato dallo IEN stesso; 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 il documento e/o il certificato cui la marca fu originariamente apposta.

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 di TSA 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.

7.7 Protezione dei documenti informatici

È stato realizzato da parte del Certificatore InfoCamere un servizio per la conservazione sicura di documenti informatici, siano essi firmati digitalmente oppure non firmati: di ogni documento archiviato viene garantita nel tempo l'immodificabilità, la reperibilità, la visualizzazione previa abilitazione.
Nel caso in cui i file siano firmati digitalmente, la procedura si fa carico, al momento dell'acquisizione del file, di marcarlo temporalmente qualora non sia già stata assegnata ad esso una marca temporale; provvede, poi, su richiesta dell'utente, ad estenderne la validità legale nel tempo, apponendovi le opportune successive marche temporali..

7.7.1 Procedure per la richiesta di conservazione di documenti informatici

L'utente che desidera conservare i propri documenti informatici potrà avvalersi del servizio indicato al § 7.7, seguendo le procedure riportate nel relativo manuale utente.
La richiesta del servizio è gestita secondo le modalità previste da apposito contratto.

7.7.2 Modalità di conservazione dei documenti informatici

L'utente, abilitato all'utilizzo del servizio suddetto può scegliere le modalità di conservazione del documento tra le due previste dall'applicazione:

- conservazione del file in formato originale
- archiviazione ottica sostitutiva a norma CNIPA

Per tutto ciò che concerne l'utilizzo dell'applicazione e le funzionalità da esso offerte relativamente la scelta delle modalità di conservazione del documento, le operazioni per la sua gestione una volta archiviato, nonché le modalità per richiederne copia, si rimanda al relativo manuale utente.

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 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 10 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

Nell'eventualità di cessazione dell'attività di certificazione, il Certificatore comunicherà questa intenzione al CNIPA con un anticipo di almeno 60 giorni, indicando 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 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.
Il Certificatore è in possesso della certificazione ISO9001 del sistema qualità aziendale.

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	Dalle 00:00 alle 24:00 dal lunedì al venerdì

(*) 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) saranno revocati i certificati per i quali risultano contemporaneamente compromessa sia la chiave di certificazione sia quella utilizzata per la generazione della marcatura temporale;
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 anno il Certificatore comunica al CNIPA la permanenza dei requisiti per l'esercizio dell'attività di certificazione e fornisce la versione aggiornata del manuale operativo.
Ogni modifica tecnica o procedurale a questo manuale operativo verrà prontamente comunicata agli Uffici di Registrazione.

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.card.infocamere.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'Area Sistemi Sicurezza Informatica e dal Responsabile Consulenza e Servizi Legali di InfoCamere S.C.p.A..

15.4 Conformità

I contenuti del presente Manuale Operativo sono pienamente rispondenti alle regole tecniche descritte nel DCPM del 13 gennaio 2004.

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 antiintrusione 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 DTS 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 devono essere chiavi RSA ed avere una 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.

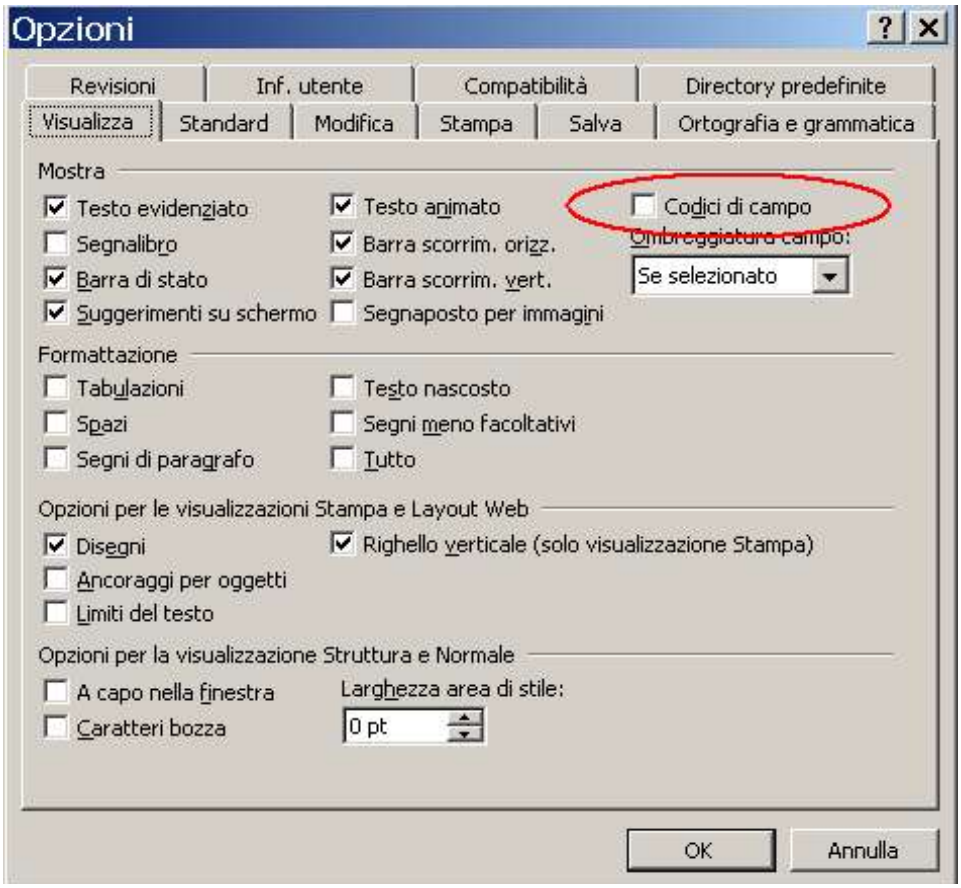
18.1 A.1 MS Word 2000 e MS Excel 2000

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 solo di macro firmate. Le macro non firmate verranno disattivate automaticamente. Una protezione **Media** consente di visualizzare la finestra di dialogo relativa alla protezione da virus macro che consente di disattivare le macro sospette.

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.



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 fa la stessa procedura e si deseleziona Formule.

18.2 A.2 Acrobat Reader 6.0

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**