Certificatore InfoCert

Certificati di Sottoscrizione di firma remota

Manuale Operativo

Codice documento: ICERT-INDI-MO-REMOTE

Questa pagina è lasciata
intenzionalmente bianca

Indice

Table of Contents

1. Introduzione al documento

Versione/Release n°:	1.0	**Data Versione/Release**:	28/05/2014
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

1.1 Proprietà Intellettuale

1.2 Cos'è il Manuale Operativo

Il presente documento descrive le regole e procedure adottate da InfoCert, in qualità di Certificatore Autorizzato, per l'emissione di certificati digitali qualificati per procedure di firma remota, denominati "Remote".
La caratteristica di detti certificati qualificati è quella di essere utilizzati nell'ambito di una particolare procedura di firma che consente al Titolare di garantire il controllo esclusivo del dispositivo di firma accedendo allo stesso con modalità a distanza.
Il presente documento, inoltre, identifica i soggetti coinvolti nel procedimento di rilascio dei certificati qualificati Remote, gli obblighi e le responsabilità di detti soggetti e degli utenti, i presupposti e le modalità di rilascio dei certificati, quelle di loro utilizzo e le procedure di sospensione e revoca degli stessi.
Il Manuale Operativo deve essere osservato dai soggetti che provvedono al rilascio dei certificati qualificati Remote, dai titolari dei medesimi e dagli utenti.
Il contenuto si basa sulle norme vigenti alla data di emissione e recepisce le raccomandazioni del documento *"Request for Comments: 2527 – Certificate Policy and certification practices framework"* © Internet Society 1999.

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

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

[2] --- non utilizzato ---

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

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

[5] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (G.U. n. 117 del 21-5-2013)]. Referenziato nel seguito come **DPCM**

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

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

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

[9] Legge 24 Dicembre 1993, n. 537

[10] Legge 23 Dicembre 1993, n. 547

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

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

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

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

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

[16] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 19 luglio 2012 - Definizione dei termini di validita' delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma. (Gazzetta Ufficiale n. 237 del 10-10-2012);

[17] Decreto Legislativo 6 settembre 2005, n.206 - Codice del Consumo

[18] Provvedimento Garante per la protezione dei dati personali 26 marzo 2003 [1053753]

[19] InfoCert - Manuale Operativo ICERT-INDI-MO per i certificati di sottoscrizione, disponibile su www.firma.infocert.it

[20] DETERMINAZIONE COMMISSARIALE N.63/2014 Oggetto: modalità di attuazione dell'articolo 19, comma 7, del DPCM 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71."

Riferimenti tecnici

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

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

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

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

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

1.4 Definizioni

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

Accreditamento facoltativo – cfr CAD – art 29

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

Autorità per la marcatura temporale *[Time-stamping authority]*
È il sistema software/hardware, gestito dal ***Certificatore***, che eroga il servizio di marcatura temporale.

Certificato, Certificato Digitale, Certificato X.509 *[Digital Certificate]*
Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.
Nel certificato compaiono altre informazioni tra cui:
- il ***Certificatore*** che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificato Qualificato – cfr. CAD

Certificato Remote
Il certificato digitale qualificato disciplinato nel presente Manuale Operativo.

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD – art 27

Certificatore Qualificato – cfr. CAD – art 29

Chiave Privata e Chiave Pubblica – cfr. CAD

Dati per la creazione di una firma – cfr. DPCM

Dati per la verifica della firma – cfr. CAD – art 28

Dispositivo sicuro per la creazione della firma (SSCD)– cfr.CAD
Il dispositivo sicuro di firma utilizzato dal ***Titolare*** è un dispositivo crittografico rispondente a requisiti di sicurezza determinati dalla legge. Per il Certificato Remote è un HSM.

Dispositivo di tipo grafometrico
Dispositivo attraverso il quale è possibile rilevare i parametri caratteristici della firma autografa (ad esempio: pressione, direzione del tratto, ecc.).

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

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

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

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

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

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

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

OTP - One Time Password
Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Titolare in un momento immediatamente antecedente all'apposizione della firma digitale. Può essere basato su dispositivi hardware o su procedure software.

Procedura di firma remota
Particolare procedura di firma elettronica qualificata o di firma digitale che consente di garantire il controllo esclusivo dei dati per la creazione della firma.

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

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

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

Regole tecniche
Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, [5].

Revoca o sospensione di un Certificato
È l'operazione con cui il ***Certificatore*** annulla la validità del certificato prima della naturale scadenza.

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

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

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

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

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

WebCam
Videocamera di ridotte dimensioni, destinata a trasmettere immagini in streaming via Internet e catturare immagini fotografiche. Collegata ad un pc e utilizzata per chat video o per videoconferenze.

1.5 Acronimi e abbreviazioni

AgID – Agenzia per l'Italia Digitale (ex-CNIPA, ex-DigitPA). Autorità di Vigilanza sui Certificatori Accreditati

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***.

ETSI - European Telecommunications Standards Institute

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

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

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

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

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

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

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

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

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

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

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

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

2. Generalità

2.1 Identificazione del Manuale Operativo

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

L'*object identifier* (OID) **1.3.76.36.1.1.35** identifica:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Manuale-operativo-firma-applicata tramite HSM (**CAD** Art. 35 comma 3, [16]) – certificati Remote	1.3.76.36.1.1.35

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

I certificati emessi sotto questa policy **possono** contenere l'OID 1.3.76.16.3 relativo a quanto indicato da AGID in [20]

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

2.2 Soggetti coinvolti nei processi

2.2.1 Certificatore

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

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Piazza Sallustio 9 00187 Roma**
Sede operativa	**Via Marco e Marcelliano 45 00147 Roma**
Rappresentante legale	**Fernando Zilio** In qualità di Presidente del Consiglio d'Amministrazione
Amministratore Delegato	
N° telefono	**06836691**
N° Iscrizione Registro Imprese	**Codice Fiscale 07945211006**
N° partita IVA	**07945211006**
Sito web	http://www.firma.infocert.it/

2.2.2 Uffici di Registrazione

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

- identificazione e registrazione del ***Titolare***,
- validazione della richiesta del certificato,
- attivazione della procedura di certificazione della chiave pubblica,

L'Ufficio di Registrazione, anche tramite suoi incaricati, svolge tutte le attività di interfaccia tra il ***Certificatore*** ed il ***Titolare***.
Gli Uffici di Registrazione sono attivati dal ***Certificatore*** a seguito di un adeguato addestramento del personale impiegato, che potrà svolgere le funzioni di identificazione, ed eventualmente registrazione, anche presso il ***Titolare***.
Il ***Certificatore*** verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo Manuale.

2.2.3 Titolare

E' il soggetto a cui è rilasciato il Certificato Qualificato e che risulta intestatario dello stesso all'interno del medesimo.

2.2.4 Richiedente

E' il soggetto che, anche attraverso il proprio sistema informatico, formalizza la richiesta di emissione del certificato qualificato trasmettendola al Certificatore e che, ove previsto negli accordi con il Certificatore, provvede al pagamento dei corrispettivi del servizio.

2.3 Applicazione e comunicazioni

2.3.1 Applicabilità

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

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

- il certificato emesso dal ***Certificatore*** sarà usato per verificare la Firma Digitale del ***Titolare*** cui il certificato appartiene.
- Il ***Certificatore*** InfoCert mette a disposizione per la verifica delle firme il prodotto descritto al §6. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

AVVERTENZA 1: l'HSM è l'unico SSCD previsto per l'utilizzo del Certificato Remote.

2.4 Contatto per utenti finali e comunicazioni

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

InfoCert S.p.A.
Responsabile Certificazione Digitale
Corso Stati Uniti 14
35127 Padova
Telefono: 06836691

Fax : 049 8288 406

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

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

2.5 Rapporti con AgID

Il presente Manuale Operativo, compilato dal Certificatore nel rispetto delle indicazioni legislative, è stato consegnato, in copia, all'Autorità di Vigilanza che lo rende disponibile pubblicamente.
Al momento della richiesta d'iscrizione, il Certificatore fornisce all'autorità di vigilanza sui certificatori i dati identificativi richiesti, che vengono da quest'ultima sottoscritti, conservati e pubblicati.

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

Il certificato relativo alle chiavi con cui viene firmato l'elenco pubblico dei certificatori accreditati è caratterizzato dall'OID 1.3.76.36.1.1.26.

3. Obblighi

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

3.1 Obblighi dei soggetti

3.1.1 Obblighi del Certificatore

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

1. siano soddisfatte tutte le regole tecniche specificate nel DPCM [5];
2. siano soddisfatte le modalità di riconoscimento del ***Titolare*** ai sensi delle norme [1], [11], [12], [13] e [15], con particolare riguardo all'identificazione dello stesso;
3. il Sistema Qualità sia conforme alle norme ISO 9001;
4. la richiesta di certificazione abbia caratteristiche di autenticità;
5. sia specificata nel certificato qualificato, su richiesta dell'istante, e con il consenso del ***Terzo Interessato*** la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;
6. la chiave pubblica di cui si richiede la certificazione non sia già stata certificata, per un altro soggetto ***Titolare***, nell'ambito del proprio dominio. Per la verifica nel dominio degli altri certificatori accreditati, il ***Certificatore*** si impegna a stabilire accordi con gli altri certificatori presenti nell'Elenco dell'Autorità di Vigilanza, in base alle attuali conoscenze tecnologiche, per l'attivazione di tali controlli;
7. sia rilasciato e reso pubblico, se esplicitamente richiesto dal ***Titolare***, il certificato qualificato secondo quanto stabilito all'art. 32, comma 3, lett. b) del **CAD**;
8. i Titolari siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi nonché riguardo agli obblighi da essi assunti in merito alla protezione della segretezza della chiave privata;
9. il proprio sistema di sicurezza dei dati sia rispondente alle misure minime di sicurezza per il trattamento dei dati personali, secondo il Decreto Legislativo 30 giugno 2003, n. 196 ;
10. il certificato sia revocato tempestivamente in caso di:
    - richiesta da parte del ***Titolare,***
    - richiesta da parte del ***Terzo Interessato***
    - richiesta da parte del ***Richiedente***
    - di compromissione della chiave privata
    - di provvedimento dell'autorità
    - d'acquisizione della conoscenza di cause limitative della capacita del ***Titolare***
    - di sospetti di abusi o falsificazioni;
11. sia certa l'associazione tra chiave pubblica e ***Titolare***;
12. il codice identificativo assegnato a ciascun ***Titolare*** sia univoco nell'ambito dei propri utenti;
13. 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 20 (venti) anni dalla data di scadenza del certificato le informazioni ottenute in fase di registrazione, di richiesta di certificazione, di revoca e di rinnovo;
15. siano custoditi per 20 (venti) anni in forma accessibile i certificati delle proprie chiavi pubbliche di certificazione;
16. alla data del rilascio siano esatte e complete le informazioni necessarie alla verifica della firma contenute nel certificato e rispetto ai requisiti fissati per i certificati qualificati
17. i dati per la creazione della firma siano sotto il controllo esclusivo del ***Titolare***.

3.1.2 Obblighi dell'Ufficio di Registrazione

L'Ufficio di Registrazione è tenuto a garantire:

1. che il ***Titolare*** sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata;
2. che il ***Titolare*** sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. 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;
4. le caratteristiche di autenticità della richiesta di certificazione;
5. la verifica dell'identità del ***Titolare*** del certificato, il controllo e la registrazione dei dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;
6. la protezione della segretezza e la conservazione degli strumenti di autenticazione utilizzati per l'attivazione ed esecuzione della procedura di registrazione;
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;
10. l'invio tempestivo al Certificatore degli originali delle richieste di certificazione.;
11. il presidio e la gestione delle procedure e degli strumenti di autenticazione al servizio di firma da parte dei Titolari, ove gestite nel proprio dominio.

L'Ufficio di Registrazione terrà direttamente i rapporti con Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Manuale Operativo.
Per il corretto riconoscimento, effettuato secondo la modalità 5 (cfr § 4.1.1), l'***Ufficio di Registrazione*** è tenuto inoltre a:

12. dotare la postazione dei propri incaricati della piattaforma di videoriconoscimento del ***Certificatore***, integrata con il sistema di videoconferenza specificatamente fornito o autorizzato;
13. eseguire la procedura di identificazione solamente in presenza di una buona qualità dell'audio e del video.

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. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo e dalle vigenti leggi nazionali e internazionali;
3. l'uso esclusivo dei dati per la generazione delle firme;
4. l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
5. di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato il certificato;
6. la richiesta di revoca o di sospensione dei certificati in suo possesso nei casi previsti dal presente Manuale Operativo;
7. di non apporre firme elettroniche avvalendosi di chiavi private basate su un certificato emesso in base ad un certificato di certificazione che a lui sia noto essere stato revocato;
8. la protezione della segretezza e la conservazione degli strumenti di autenticazione utilizzati per l'attivazione della procedura di firma;

9. la protezione della segretezza e conservazione del codice di emergenza per richiedere la sospensione del proprio certificato;
10. di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato il certificato.

3.1.4 Obblighi degli Utenti

L'utente che riceve e utilizza un documento informatico firmato dal Titolare, che quindi contiene il certificato, 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, possibilmente al momento della generazione della firma, controllando le relative liste nel registro dei certificati.
3. Verificare il rispetto dei limiti d'uso eventualmente inseriti nel certificato;
4. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.1.5 Obblighi del Terzo Interessato

Il ***Terzo Interessato***, che, **avendo presa visione del presente Manuale Operativo**, manifesta il proprio consenso all'inserimento nel certificato di un Ruolo oppure autorizza o richiede l'indicazione dell'Organizzazione a cui il ***Titolare*** e collegato, e tenuto a:
1. attenersi a quanto disposto dal presente Manuale Operativo;
2. provvedere tempestivamente all'inoltro della richiesta di revoca o sospensione nei casi previsti dal presente Manuale Operativo.

3.1.6 Obblighi del Richiedente

Il ***Richiedente*** che, **avendo presa visione del presente Manuale Operativo**, acquisisce i certificati qualificati e formalizza le richieste di emissione dei Titolari è tenuto a:
1. attenersi a quanto disposto dal presente Manuale Operativo;
2. provvedere tempestivamente all'inoltro della richiesta di revoca o sospensione nei casi previsti dal presente Manuale Operativo.

3.2 Limitazioni e indennizzi

3.2.1 Limitazioni della garanzia e limitazioni degli indennizzi

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

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

3.3 Pubblicazione

3.3.1 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 elettronico presso l'Ufficio di Registrazione
- 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'Autorità di Vigilanza.

3.3.2 Pubblicazione dei certificati

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

3.3.3 Pubblicazione delle liste di revoca e sospensione

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

3.4 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.

3.5 Tutela dei dati personali

Le informazioni relative al ***Titolare*** 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.

3.6 Tariffe

Le tariffe per l'acquisizione di questi certificati saranno incluse nel contratto del servizio ai cui fini questi certificati vengono rilasciati.

3.6.1 Accesso al certificato e alle liste di revoca

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

4. Modalità di identificazione e registrazione

Questo capitolo descrive le procedure usate per l'identificazione del ***Titolare*** ai fini del rilascio del Certificato Remote.

4.1 Modalità di identificazione

Il ***Certificatore*** deve verificare l'identità del ***Titolare*** prima di procedere al rilascio del certificato di sottoscrizione richiesto.

4.1.1 Soggetti abilitati ad effettuare l'identificazione

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

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

Modalità 2
Intermediari finanziari e altri soggetti esercenti attività finanziaria.

Modalità 3
Identificazione tramite firma digitale.

Modalità 4
Identificazione tramite CNS/CIE.

Modalità 5
1. Il ***Certificatore***, anche tramite i suoi incaricati, supportati da un sistema di videoconferenza
2. L'***Ufficio di Registrazione***, anche tramite i suoi incaricati, supportati da un sistema di videoconferenza

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 1

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

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

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

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purche munite di fotografia edi timbro, rilasciate da un'Amministrazione dello Stato.
Al momento dell'identificazione viene fornito al ***Titolare*** un codice emergenza, che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra ***Certificatore*** e ***Titolare*** (cfr. art. 17 **DPCM**).
L'identificazione da parte dei Pubblici Ufficiali (cfr. Appendice B) puo essere altresi effettuata in base a quanto disposto dalle normative che disciplinano la loro attivita, ivi comprese le disposizioni di cui al [15] e successive modifiche ed integrazioni.

4.1.2.2 Riconoscimento effettuato secondo la modalità 2

Nella **modalità 2** il ***Certificatore*** si avvale del riconoscimento già effettuato da un Intermediario finanziario o da altro Soggetto Esercente Attività Finanziaria, che, ai sensi delle norme antiriciclaggio tempo per tempo vigenti, è obbligato al riconoscimento dei propri clienti.
I dati utilizzati per il riconoscimento sono rilasciati dal ***Titolare*** ai sensi del D.Lgs. 231/07, a norma del quale i clienti sono tenuti a fornire - sotto la propria responsabilità - tutte le informazioni necessarie e aggiornate per consentire agli Intermediari e agli altri Soggetti Esercenti Attività Finanziaria di adempiere agli obblighi di identificazione della clientela.
Gli Intermediari e gli altri Soggetti Esercenti Attività Finanziaria acquisiscono i Dati in base alle procedure alle adottate ai sensi degli articoli 19, co. 1 lettera a) (identificazione e verifica dell'identità del cliente in sua presenza), 22 (modalità di attuazione degli obblighi di adeguata verifica nei confronti dei nuovi clienti e della clientela già acquisita), 28 (identificazione e verifica dell'identità del cliente, anche in sua assenza, mediante l'adozione di misure rafforzate di adeguata verifica), 29 e 30 (identificazione e verifica dell'identità del cliente, anche in sua assenza, in quanto dette attività vengono effettuate da parte di terzi) del D.Lgs. 231/2007, e ss.mm.ii.; ovvero alle analoghe procedure adottate secondo la normativa antiriciclaggio vigente alla data del riconoscimento al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale).
In questo caso, previo apposito accordo con l'Intermediario finanziario, **che agisce da Ufficio di Registrazione**, i dati identificativi del ***Titolare*** raccolti da quest'ultimo all'atto del riconoscimento vengono utilizzati direttamente per l'emissione dei certificati, previa accettazione da parte del ***Titolare*** delle condizioni contrattuali per il rilascio del certificato e degli strumenti per l'apposizione della firma nonché approvazione e conferma dei dati anagrafici registrati.

4.1.2.3 Riconoscimento effettuato secondo la modalità 3

Nella **modalità 3** il ***Certificatore*** si basa sul riconoscimento già effettuato da un altro ***Certificatore.*** Il ***Titolare*** è già in possesso di un dispositivo di firma con un certificato qualificato a bordo ancora in corso di validità. Il ***Titolare*** inoltra alla CA la richiesta di emissione del Certificato Remote, firmata digitalmente, tramite l'Ufficio di Registrazione.
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.2.4 Riconoscimento effettuato secondo la modalità 4

Nella **modalità 4** il ***Certificatore*** si basa sul riconoscimento già effettuato da un Ente Emettitore di CNS o dal Comune che ha rilasciato la CIE**.** Il ***Titolare,*** già in possesso di un dispositivo sicuro con un certificato CIE o CNS ancora in corso di validità, si autentica al portale del Certificatore o dell'Ufficio di Registrazione ed inoltra la richiesta di emissione del Certificato Remote.
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.2.5 Riconoscimento effettuato secondo la modalità 5

Nella **modalità 5** l'identificazione e effettuata da uno dei soggetti indicati al §4.1.1 (Modalita 1) e sono richiesti, da parte del ***Titolare,*** il possesso di un pc, una webcam ad esso collegata e un sistema audio pc funzionante.
Il soggetto che effettua l'identificazione verifica l'identita del ***Titolare*** tramite il riscontro con un documento di riconoscimento in corso di validità, purche munito di fotografia recente e riconoscibile del ***Titolare***, firma autografa del ***Titolare*** e di timbro, rilasciato da un'Amministrazione dello Stato. E' facoltà del soggetto che effettua l'identificazione escludere l'ammissibilità del documento utilizzato dal ***Titolare*** se ritenuto carente delle caratteristiche elencate.
Al ***Titolare*** viene fornito un codice emergenza, che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra ***Certificatore*** e ***Titolare*** (cfr. art. 17 DPCM).
I dati identificativi del ***Titolare***, confermati all'atto del riconoscimento, vengono utilizzati per l'emissione dei certificati, previa accettazione da parte del ***Titolare*** delle condizioni contrattuali e del trattamento dei dati personali, per il rilascio del certificato e degli strumenti per l'apposizione della firma nonche approvazione e conferma dei dati anagrafici registrati. I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, vengono conservati in forma protetta per una durata ventennale, secondo quanto indicato nell'art. 32, comma 1, lettera j) del CAD.
La procedura in uso soddisfa quanto richiesto dall'art. 32, comma 1, lettera a) del CAD.

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

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

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

4.1.4 Informazioni che il Titolare deve fornire

Nella richiesta di registrazione sono contenuti sia i dati relativi all'identità del cliente che le informazioni che consentono di gestire in maniera efficace il rapporto tra il ***Certificatore*** ed il ***Titolare***.

Sono considerate **obbligatorie** le seguenti informazioni:
- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale o analogo codice identificativo[1]
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, ove presente, quali tipo, numero, ente emittente e data di rilascio dello stesso
- e-mail per l'invio delle comunicazioni dal ***Certificatore*** al ***Titolare***.

Opzionalmente il ***Titolare*** può fornire un altro nome, con il quale è comunemente conosciuto, che sarà inserito in un apposito campo denominato *commonName* (nome comune) del SubjectDN del certificato.

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

Il commonName, nel caso in cui non venisse fornito alcun ulteriore nome dal ***Titolare***, sarà valorizzato con nome e cognome del ***Titolare*** stesso.

4.1.5 Uso di pseudonimi

E' facolta del ***Titolare*** richiedere al ***Certificatore*** che il certificato riporti uno pseudonimo in luogo dei propri dati reali. Poiche il certificato e qualificato il ***Certificatore*** conserverà le informazioni relative alla reale identita dell'utente per venti (20) anni dopo la scadenza del certificato stesso.
L'uso dello pseudonimo NON è consentito per il riconoscimento nella modalità 3 del presente paragrafo 4.

4.1.6 Limiti d'uso e limiti di valore

Per i certificati emessi sotto questa policy non è previsto l'inserimento di limiti di valore.

Per quanto riguarda i limiti d'uso, il Certificato Remote è limitato nel suo utilizzo nell'ambito di un determinato dominio applicativo o per i rapporti con un determinato soggetto o per la sottoscrizione di tipologie documentali specifiche.

Nel certificato è quindi riportato il seguente limite d'uso:

Il certificato è usabile solo nei rapporti tra titolare e richiedente. The certificate can be used only in the relationships between the holder and the requestor.

I Certificati Remote possono essere rilasciati anche con la seguente limitazione d'uso:
Uso limitato alla firma di documenti informatici dell'Organizzazione indicata nel campo Organization del certificato per l'esercizio delle funzioni relative al ruolo ricoperto dal Titolare.

Ferma restando la responsabilità del ***Certificatore*** di cui al **CAD** (art.30 comma 1 lettera a), è responsabilità dell'**Utente** verificare il rispetto dei limiti d'uso inseriti nel certificato.
La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dal ***Certificatore*** per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.
Oltre ai limiti suddetti, il ***Certificatore*** adotta i limiti d'uso pubblicati sul sito dell'autorità di Vigilanza che compariranno nel certificato come ulteriori Certificate Policy, cosi identificati:

1.3.76.36.1.1.23	I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
1.3.76.36.1.1.24.1	Il presente certificato è valido solo per firme apposte con procedura automatica. La presente dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati
1.3.76.36.1.1.24.2	The certificate may be used only for automatic procedure signature purposes.
1.3.76.36.1.1.25	L'utilizzo del certificato è limitato ai rapporti con *(indicare il soggetto)*. The certificate may be used only for relations with the *(declare the subject)*.

4.1.7 Inserimento del Ruolo e dell'Organizzazione nel certificato

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

In questo caso, il ***Titolare***, oltre alla documentazione e alle informazioni identificative necessarie (cfr. §4.1.2, §4.1.4), dovrà produrre anche quella idonea a dimostrare l'effettiva sussistenza dello specifico

Ruolo anche attestandolo, ove espressamente consentito dal presente Manuale Operativo, mediante Autocertificazione, ai sensi dell'art. 46 del D.P.R. 445/2000.

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

La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione potranno essere invece riportate nel Certificato Remote a fronte di apposito accordo con il Certificatore, qualora detta organizzazione ricopra la qualifica di ***Richiedente*** o di ***Terzo Interessato***, anche senza l'esplicita indicazione di un ruolo.
In tale ipotesi il ***Certificatore*** effettua un controllo sulla regolarità formale della documentazione presentata dal ***Titolare***.
La richiesta di Certificati Remote con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni in possesso di Codice Fiscale.

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

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

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

Il certificato con il Ruolo è conforme a quanto indicato nella Deliberazione CNIPA [4].

4.1.7.1 Titoli e/o Abilitazioni Professionali

Nel caso in cui sia richiesta l'indicazione nel Certificato Remote di Abilitazioni Professionali per l'esercizio delle quali sia necessario ottenere preventivamente l'iscrizione all'Albo su verifica dell'Ordine professionale competente alla tenuta e vigilanza dello stesso, il ***Titolare***, salvo diversa pattuizione tra il ***Certificatore*** e l'Ordine di appartenenza, dovrà fornire un certificato rilasciato dall'Ordine, o un'autocertificazione ai sensi dell'art. 46 del D.P.R. n. 445/2000, ed il consenso scritto da parte di quest'ultimo manifestato sull'apposito modulo fornito dal ***Certificatore***.
La documentazione da presentare ai sensi dei commi precedenti non dovrà essere anteriore di oltre 10 (dieci) giorni alla data della richiesta di registrazione.
Il ***Certificatore*** si riserva di subordinare l'inserimento nel certificato delle informazioni che rientrano in questa categoria alla stipulazione di appositi accordi con i singoli enti, cui compete la gestione e tenuta degli albi, elenchi e/o registri professionali, per la disciplina delle modalità di attestazione del Ruolo del ***Titolare*** e l'adempimento di quanto previsto a loro carico in qualità di ***Terzo Interessato***.
Per l'esercizio delle professioni per le quali sia richiesto l'iscrizione ad appositi albi non soggetti al controllo e verifica da parte di un apposito ente, il ***Titolare*** potrà attestare eventuali titoli mediante Autocertificazione, ai sensi dell'art. 46 D.P.R. 445/2000

4.1.7.2 Poteri di rappresentanza di persone fisiche

Nel caso in cui sia richiesta l'indicazione nel certificato di un Ruolo relativo alla *Rappresentanza di persona fisica,* il ***Titolare*** dovrà fornire, all'atto dell'identificazione, la copia autentica della delega o procura notarile sottoscritta dalla persona rappresentata e l'attestazione di consenso di quest'ultima all'inserimento del Ruolo nel certificato; nei casi previsti dalla legge, la prescritta documentazione potrà essere costituita da copia autentica del provvedimento emesso dall'autorità giudiziaria competente.
Il ***Titolare*** dovrà fornire altresì gli elementi di cui al paragrafo §4.1.4 relativi anche al rappresentato, escluse le informazioni relative alle modalità di comunicazione tra ***Certificatore*** e ***Titolare*** indicate nell'ultimo punto dell'elenco.

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

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

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

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

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

- nome e cognome,
- codice fiscale,
- numero di telefono presso l'organizzazione,
- l'indirizzo di posta elettronica presso l'organizzazione,
- il Ruolo da inserire nel certificato.
- La lettera dell'ente di appartenenza deve contenere una dichiarazione che **impegna** l'organizzazione a **comunicare tempestivamente** al ***Certificatore*** ogni variazione alle informazioni sopra elencate.

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

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

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

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

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

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

4.2 Autenticazione per rinnovo delle chiavi e certificati

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

NOTA

le date indicate negli attributi suddetti sono espresse nel formato

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

nella rappresentazione UTCTime prevista dallo standard di riferimento [16]

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

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

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

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

4.3 Autenticazione per richiesta di Revoca o di Sospensione

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

4.3.1 Richiesta da parte del Titolare

Se la richiesta viene effettuata per telefono o via Internet, il ***Titolare***, esclusivamente per la funzione di sospensione, si autentica fornendo il codice di emergenza, consegnato assieme al certificato che

intende sospendere, oppure altro sistema di autenticazione descritto nella documentazione contrattuale consegnata all'atto della registrazione.
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 7.1.2.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del ***Terzo Interessato*** in apposite convenzioni da stipulare con lo stesso.

4.3.3 Richiesta da parte del *Richiedente*

Il ***Richiedente*** che richiede la revoca o sospensione del certificato del ***Titolare***, si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal ***Certificatore*** e munendolo, qualora si tratti di un ente, di timbro o altra segnatura equivalente.
La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 7.1.2.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del ***Richiedente*** in apposite convenzioni da stipulare con lo stesso.

5. Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione 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, anche telematicamente.

Conclusasi la fase di registrazione iniziale, il rilascio del Certificato Remote è previsto in unica modalità, ossia con chiavi generate su dispositivi HSM.

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

Le modalità di registrazione del ***Titolare*** e di identificazione dello stesso sono diverse in base ai rapporti tra ***Titolare*** ed ***Ufficio di Registrazione***.

Per la conferma delle operazioni di rilascio al ***Titolare*** verrà richiesto l'utilizzo di un dispositivo di autenticazione.

5.2 Rilascio del certificato

5.2.1 Caso A: Rilascio in presenza del Titolare

La procedura si applica nei casi in cui il ***Titolare*** è identificato da un ***Ufficio di Registrazione*** o un Pubblico Ufficiale in presenza, ai sensi della Modalità 1 o 2 di identificazione. In questo secondo caso l'Ufficio di Registrazione è un Intermediario Finanziario o un Soggetto Esercente Attività Finanziaria.

- Il ***Titolare*** contatta l'***Ufficio di Registrazione***, che procede ad attestarne l'identità in presenza sulla base dei documenti di identità;
- Il ***Titolare*** si collega al sito dell'***Ufficio di Registrazione*** e richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici, che eventualmente può essere già precompilato con i dati del ***Titolare*** inseriti dall'***Ufficio di Registrazione stesso***;
- Il ***Titolare*** conferma i propri dati ed inserisce eventuali aggiornamenti dei medesimi;
- Il ***Titolare*** manifesta la volontà di ottenere il rilascio di un certificato digitale mediante conferma ed accettazione della richiesta di registrazione sulla procedura web. L'***Ufficio di Registrazione*** – che può ricoprire anche la qualifica di ***Richiedente*** – produce un'evidenza informatica, con cui attesta le caratteristiche di veridicità della richiesta di rilascio, e la trasmette al Certificatore;
- L'***Ufficio di Registrazione*** comunica la corretta identificazione del *Titolare* al certificatore, che provvede al rilascio del certificato.

5.2.2 Caso B: Rilascio da remoto

La procedura si applica nei casi in cui il ***Titolare*** si collega da remoto alla procedura dell'***Ufficio di Registrazione***, che provvede all'identificazione ai sensi della Modalità 2 qualora sia un Intermediario Finanziario o un Soggetto Esercente Attività Finanziaria, ovvero si avvale alternativamente delle Modalità di identificazione 3, 4 o 5.

5.2.2.1. Ipotesi 1: il Titolare è un cliente attivo

In presenza di un rapporto contrattuale continuativo dell'***Ufficio di Registrazione*** con il ***Titolare*** il rilascio del certificato Remote avviene secondo la seguente procedura.

1) Il ***Titolare*** si collega al sito dell'***Ufficio di Registrazione*** e richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici (se il ***Titolare*** ha già un rapporto in essere con l'***Ufficio di Registrazione*** (Cliente Attivo) si autentica con le credenziali precedentemente fornite dall'***Ufficio di Registrazione*** stesso, il form risulta precompilato con i dati del cliente);
2) Il ***Titolare*** conferma i propri dati ed inserisce eventuali aggiornamenti dei medesimi;
3) Il ***Titolare*** manifesta la volontà di ottenere il rilascio di un certificato digitale mediante conferma sulla procedura web. L'***Ufficio di Registrazione*** produce un'evidenza informatica, con cui attesta le caratteristiche di veridicità della richiesta di rilascio, e la trasmette al certificatore;
4) L'***Ufficio di registrazione***, qualora Intermediario Finanziario o un Soggetto Esercente Attività Finanziaria, verifica la rispondenza dei dati inseriti dal Cliente Attivo con quelli presenti presso i propri archivi raccolti sulla base del riconoscimento svolto ai sensi del D.L.vo n. 231/2007 e ss.mm.ii. Qualora i dati corrispondano ad un ***Titolare*** già registrato e non ci sia stata autenticazione, viene richiesta in questa fase.
   4.1 In caso di corrispondenza dei dati comunica la corretta identificazione del ***Titolare*** al ***Certificatore***, che provvede al rilascio del certificato qualificato;
   4.2 In caso di mancata corrispondenza non viene dato seguito alla richiesta di certificazione;
5) Nel caso in cui l'***Ufficio di registrazione*** non rivesta la qualità di Intermediario Finanziario o Soggetto Esercente Attività Finanziaria, inizia la procedura di identificazione da remoto tramite la Modalità 3, la Modalità 4 o la Modalità 5;
6) Dopo il corretto completamento della procedura di identificazione, il ***Certificatore*** provvede all'emissione del Certificato Remote.

5.2.2.2. Ipotesi 2: il Titolare non è un cliente attivo (prospect)

In assenza di un rapporto contrattuale continuativo dell'***Ufficio di Registrazione*** con il ***Titolare*** il rilascio del certificato Remote avviene secondo la seguente procedura.

1) Il ***Titolare*** si collega al sito dell'***Ufficio di Registrazione*** e richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici;
2) Il ***Titolare*** conferma i propri dati ed inserisce eventuali aggiornamenti dei medesimi;
3) L'***Ufficio di Registrazione*** inizia la procedura di identificazione da remoto tramite la Modalità 2, la Modalità 3, la Modalità 4 o la Modalità 5;
4) Il ***Titolare*** manifesta la volontà di ottenere il rilascio di un certificato digitale Remote mediante conferma sulla procedura web. L'***Ufficio di Registrazione*** che ha raccolto la richiesta del certificato produce un'evidenza informatica, con cui attesta le caratteristiche di veridicità della richiesta di rilascio, e la trasmette al ***Certificatore***;
5) Dopo il corretto completamento della procedura di identificazione, il ***Certificatore*** conclude il processo di emissione del Certificato Remote.

5.2.3 Generazione delle chiavi

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

5.2.4 Protezione delle chiavi private

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

5.3 Emissione del certificato

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

1) viene verificata la correttezza della richiesta di certificato controllando che:
   - la richiesta provenga da un Ufficio di Registrazione autenticato;
   - il ***Titolare*** sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - al ***Titolare*** sia stato assegnato un codice identificativo unico nell'ambito degli utenti del ***Certificatore*** (IUT);
   - la chiave pubblica che si intende certificare sia una chiave valida, della lunghezza prevista e non sia già stata certificata per un altro ***Titolare***;
   - la coppia di chiavi funzioni correttamente;
2) si procede alla generazione del certificato
3) viene attestato il momento di generazione del certificato utilizzando quale riferimento temporale la data fornita dal sistema della Certification Authority e tale registrazione viene riportata sul giornale di controllo.
4) il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati;
5) il certificato viene memorizzato nei server del sistema di emissione.

5.3.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni relative al ***Titolare*** ed indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme a quanto specificato nella Deliberazione CNIPA [4]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.
Il certificato è qualificato ai sensi della normativa vigente.

5.3.2 Pubblicazione del certificato

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

5.3.3 Validità del certificato

Il periodo di validità del certificato è determinato sulla base:

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

Alla data tale periodo non può superare i 5 (cinque) anni.

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

6. Modalità per la sottoscrizione di documenti e verifica della firma

Il Certificato Remote risiede presso un HSM gestito dal ***Certificatore***. I dati per la creazione della firma sono suddivisi in modo che unicamente attraverso la componente nota al ***Titolare*** possa essere apposta la firma qualificata su documenti informatici.

L'apposizione di firma digitale si configura come un **servizio online**, accessibile via rete (Internet). La coppia delle chiavi crittografiche e il certificato digitale, che risiede in modalita sicura nel SSCD (HSM) sito presso il ***Certificatore*** sono accessibili da remoto con modalita sicure. Il ***Titolare*** viene identificato dal servizio ed autorizza l'apposizione della firma tramite un meccanismo di sicurezza.

6.1 Modalità di autenticazione per l'attivazione della firma remota.

Il dispositivo sicuro centralizzato, Hardware Security Module (HSM), è attivabile esclusivamente dal ***Titolare*** solo a seguito di un'autenticazione forte, effettuata mediante l'utilizzo di strumenti di autenticazione forte **a due fattori** (hardware, software o un Sistema biometrico di autenticazione).
In questo contesto operativo, al momento della sua identificazione e registrazione, al ***Titolare*** viene associato un dato identificativo verificabile mediante un'autenticazione forte.
Nell'operazione di firma, il ***Titolare*** appone la propria firma mediante un applicativo realizzato dal ***Richiedente*** o, in alternativa, utilizzando un'apposita versione del software di firma e verifica distribuito dal ***Certificatore***. In entrambi i casi sono previste almeno le seguenti fasi:

- presentazione al ***Titolare*** del documento da sottoscrivere, **previa autenticazione** che ne garantisca il diritto ad accedervi;
- autenticazione forte del Titolare mediante una delle modalità sopracitate per accedere i dati per la creazione della firma;
- conferma della volontà di apporre la firma remota tramite inserimento di un codice PIN e di un OTP oppure di dati biometrici;
- generazione dell'impronta del documento e sua sottoscrizione con le chiavi custodite mediante HSM;
- chiusura del documento sottoscritto.

In base alla modalità di autenticazione forte utilizzata, sono previste differenti tipologie di attivazione e utilizzo del servizio, come descritto di seguito.
In caso di Sistema biometrico di autenticazione al momento della registrazione, al ***Titolare*** viene associato un insieme di informazioni caratteristiche della sua firma autografa, rilevate da un apposito dispositivo di tipo grafometrico.
Nella fase di autenticazione forte dell'operazione di firma, il ***Titolare*** dovrà apporre su un dispositivo grafometrico la propria firma autografa per consentire al Certificatore di verificarne la corrispondenza alle informazioni rilevate per essa al momento della registrazione.

6.1.1 Credenziali gestite dal Certificatore.

Il ***Certificatore*** ha predisposto per il Certificato Remote un sistema di gestione dinamico delle credenziali che richiede, per l'apposizione della firma remota, l'autenticazione del ***Titolare*** e, successivamente, la conferma della volontà di firmare (mediante l'utilizzo di OTP e PIN) o l'utilizzo di un Sistema biometrico di autenticazione.

La OTP è generata randomicamente dal sistema del ***Certificatore*** al momento dell'attivazione da parte del Titolare della procedura di firma remota.

La OTP viene trasmessa al ***Titolare*** tramite lo strumento hardware o software dallo stesso prescelto al momento della registrazione.

Con l'inserimento della OTP il ***Titolare*** avvia la procedura di firma remota provvedendo ad trasmettere il dato per la creazione della firma di sua esclusiva conoscenza, avviando così la procedura di Firma Digitale.

In caso di Sistema biometrico di autenticazione al momento della registrazione, al ***Titolare*** viene associato un insieme di informazioni caratteristiche della sua firma autografa, rilevate da un apposito dispositivo di tipo grafometrico.
Nella fase di autenticazione forte dell'operazione di firma, il ***Titolare*** dovrà apporre su un dispositivo grafometrico la propria firma autografa per consentire al ***Certificatore*** di verificarne la corrispondenza alle informazioni rilevate per essa al momento della registrazione.

6.1.2 Credenziali gestite dall'Ufficio di Registrazione.

Il dato per la creazione della firma, necessario per l'attivazione della firma remota, può coincidere con delle componenti di un sistema di autenticazione gestito e verificato dall'***Ufficio di Registrazione***.

In tale ipotesi il ***Certificatore*** provvede a verificare la rispondenza dei requisiti di sicurezza del sistema gestito dall'***Ufficio di Registrazione***, assicurandosi che tale sistema garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del ***Titolare***.

Il ***Titolare*** , in questo caso, utilizza la componente di credenziale o il sistema di autenticazione già in essere presso l'Ufficio di Registrazione, provvedendo ad avviare la procedura di firma remota mediante l'inserimento di tale componente direttamente sul sistema dell'***Ufficio di Registrazione*** che trasmette l'informazione alla procedura di firma remota, avviando così la procedura di Firma Digitale.

6.2 Modalità di verifica della firma.

I documenti sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF, formato di sottoscrizione previsto dall'Art.21 comma 8 e 15 della Deliberazione CNIPA n. 45.

Il formato di firma è conforme allo standard PadES (PDF Advanced Electronic Signatures) il quale non richiede la variazione dell'estensione del file ".pdf". La verifica può pertanto essere effettuata utilizzando il software Adobe Reader scaricabile gratuitamente dal sito www.adobe.com/it.

La verifica dei documenti sottoscritti potrà inoltre essere eseguita con il prodotto Dike gratuitamente scaricabile dai Titolari dal sito www.firma.infocert.it. Dike consente:

- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Deliberazione CNIPA [4].
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Circolare AIPA 24/2000 [14].

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

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

NOTA BENE: Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalita che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD. E' cura del ***Titolare*** assicurarsi, tramite le funzionalita tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.
In Appendice sono riportate le modalita 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 e 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. Revoca e sospensione di un certificato

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.
I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal ***Certificatore***, emessa e pubblicata nel registro dei certificati con periodicità prestabilita.
Il ***Certificatore*** può forzare un'emissione non programmata della CRL in circostanze particolari.
L'efficacia della revoca e della sospensione si ha dal momento di pubblicazione della lista, attestato dalla data apposta alla registrazione dell'evento nel Giornale di Controllo del ***Certificatore***.

7.1.1 Motivi per la revoca di un certificato

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

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
   - sia venuta meno la segretezza o integrità degli strumenti di autenticazione utilizzati per la procedura di firma remota;
   - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
2. 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;
3. termina il rapporto tra il ***Titolare*** e il ***Certificatore***;
4. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

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

7.1.2 Procedura per la richiesta di revoca

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

7.1.2.1 Revoca su iniziativa del Titolare

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

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

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

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

7.1.2.2 Revoca su iniziativa del Certificatore

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

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

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

7.1.2.3 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 dovra essere inoltrata per lettera o per fax, corredata di una fotocopia di un documento di identita in corso di validita.
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.
Il ***Certificatore*** si riserva di individuare ulteriori modalita di inoltro della richiesta di revoca/sospensione del ***Terzo Interessato*** in apposite convenzioni da stipulare con lo stesso.

7.1.2.4 Richiesta da parte del *Richiedente*

Il ***Richiedente*** che richiede la revoca o sospensione del certificato del ***Titolare***, si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal ***Certificatore*** e munendolo, qualora si tratti di un ente, di timbro o altra segnatura equivalente.
Il Richiedente deve fornire la motivazione della richiesta di revoca, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato.
La richiesta dovrà essere corredata di una fotocopia di un documento di identità in corso di validità.
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.
Il ***Certificatore*** si riserva di individuare ulteriori modalita di inoltro della richiesta di revoca/sospensione del ***Richiedente*** in apposite convenzioni da stipulare con lo stesso.

7.1.3 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 salvo quanto previsto al § 7.1.4.
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.

7.1.4 Motivi per la Sospensione di un certificato

Il ***Certificatore*** esegue la sospensione del certificato su propria iniziativa o per richiesta del ***Titolare,*** del ***Terzo Interessato*** o del ***Richiedente.***
La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il ***Titolare***, il ***Terzo Interessato*** o il ***Certificatore*** acquisiscano elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione della validità del certificato.

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

7.1.5 Procedura per la richiesta di Sospensione

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

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

Sono previsti i seguenti casi:

7.1.5.1 Sospensione su iniziativa del Titolare

Il ***Titolare*** si autentica fornendo il codice di emergenza, trasmesso all'email indicata al momento della registrazione oppure altro sistema di autenticazione utilizzato per la procedura di firma remota.
Se la richiesta viene fatta presso l'Ufficio di Registrazione, l'autenticazione del ***Titolare*** avviene con le modalita previste per l'identificazione.
Il Titolare può richiedere la sospensione con una delle seguenti modalità:

1. utilizzando la funzione di sospensione disponibile nel sito Web del ***Certificatore***. Per effettuare la richiesta il ***Titolare*** **deve** comunicare:
    1. i propri dati identificativi,
    2. l'identificativo univoco a lui assegnato (IUT),
    3. la motivazione,
    4. la data di fine sospensione,
    5. il codice di emergenza;
2. utilizzando (ove disponibile) la funzione di sospensione, previo utilizzo del sistema di autenticazione già in essere per la procedura di firma remota, sul sito Web indicato nella documentazione contrattuale fornita all'atto della Registrazione. Per effettuare la richiesta il ***Titolare*** **deve** autenticarsi secondo le modalità previste e comunicare:
    1. i propri dati identificativi,
    2. l'identificativo univoco a lui assegnato (IUT),
    3. la motivazione,
    4. la data di fine sospensione,
3. telefonando al Call Center del ***Certificatore*** e fornendo le informazioni di cui al punto precedente. In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una **sospensione immediata** del certificato per una durata di **10 (dieci) giorni solari** in attesa della richiesta scritta del ***Titolare***; qualora il ***Certificatore***, direttamente o tramite

un Ufficio di Registrazione, non riceva la richiesta sottoscritta entro il termine indicato, il certificato verrà riattivato.
4. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione al ***Certificatore***.

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

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

7.1.5.2 Sospensione su iniziativa del Certificatore

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

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

7.1.5.3 Sospensione su iniziativa del Terzo Interessato

La richiesta di sospensione su iniziativa del ***Terzo Interessato*** deve essere effettuata secondo la seguente modalità:
1. il ***Terzo Interessato*** richiede al ***Certificatore*** per iscritto la sospensione del certificato, compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato, la decorrenza e la data di termine della sospensione. Il Terzo Interessato è tenuto ad autenticarsi munendo il modulo di richiesta, qualora si tratti di un ente, di timbro o altra segnatura equivalente. La richiesta dovra essere inoltrata per lettera o per fax, corredata di una fotocopia di un documento di identita in corso di validità;
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***.

7.1.5.4 Sospensione su iniziativa del Richiedente

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

1. il ***Richiedente*** richiede al ***Certificatore*** per iscritto la sospensione del certificato, compilando l'apposito modulo messo a disposizione dal ***Certificatore*** stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato, la decorrenza e la data di termine della sospensione. Il Richiedente è tenuto ad autenticarsi munendo il modulo di richiesta, qualora si tratti di un ente, di timbro o altra segnatura equivalente. La richiesta dovra essere inoltrata per lettera o per fax, corredata di una fotocopia di un documento di identita in corso di validità;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare*** secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato inserendolo nella lista di revoca e sospensione (CRL).

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

7.1.6 Ripristino di validità di un Certificato sospeso

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

7.1.7 Pubblicazione e frequenza di emissione della CRL

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

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

7.1.8 Tempistica

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

7.2 Sostituzione delle chiavi e rinnovo del Certificato

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

8. Rinvio

Per quanto non espressamente previsto si vedano i paragrafi 7, 8, 9, 10, 11, 12, 13, 14, 15 e 16 del Manuale Operativo ICERT-INDI-MO [[19]] a cui espressamente si rinvia.

9. Appendice: Macroistruzioni

A.2 Acrobat Reader

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

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