Zucchetti

Autorità di Certificazione

Certificati di Sottoscrizione
Manuale Operativo

Firmato da:PAOLO CAMIA
Organizzazione:ZUCCHETTI S.P.A./05006900962
Unita':LODI VIA SOLFERINO 1
Data: 23/03/2017 14:50:17
Limite d'uso:Explicit Text: Uso limitato alla firma di documenti informatici dell'Organizzazione i
ndicata nel campo Organization del certificato per l'esercizio delle funzioni relativ
e al ruolo ricoperto dal Titolare. Explicit Text: The certificate holder must use t

Firmato da:
AgID
Certificato emesso da: AgID, Agenzia per l'Italia Digitale, IT
Riferimento temporale 'SigningTime': 19-04-2017 09:48:56
Approvo il documento

Questa pagina è lasciata
intenzionalmente bianca

Indice

1 Introduzione al documento

Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.0	**Data Versione/Release**:	20/07/15
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

Versione/Release n°:	1.1	**Data Versione/Release**:	18/09/15
Descrizione modifiche:	Inserite date di conseguimento certificazioni ISO 9001 ed ISO 27001 Estesi i limiti d'uso garantiti agli utenti Eliminato il supporto dei certificati di ruolo nel caso di poteri di rappresentanza di persone fisiche		
Motivazioni:	Seconda emissione		

Versione/Release n°:	1.2	**Data Versione/Release**:	02/10/15
Descrizione modifiche:	Eliminati i riferimenti agli accordi di cross certificazione Aggiornati i riferimenti al call center Aggiornati i limiti d'uso garantiti agli utenti		
Motivazioni:	Terza emissione		

Versione/Release n°:	1.3	**Data Versione/Release**:	14/06/16
Descrizione modifiche:	Modalità di riconoscimento, normativa, definizioni, capitolo 7		
Motivazioni:	Aggiornato per adempimento normativa EIDAS		

Versione/Release n°:	1.4	**Data Versione/Release**:	21/11/16
Descrizione modifiche:	Rilascio telematico, disponibilità servizio		
Motivazioni:	Quinta emissione		

Versione/Release n°:	1.5	**Data Versione/Release**:	20/03/17
Descrizione modifiche:	Nuovo OID dedicato alla firma remota basata su HSM, aggiornamento appendice C		
Motivazioni:	Sesta emissione		

1.1 Scopo e campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dalla autorità di certificazione **Zucchetti** 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.
Il contenuto si basa sulle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 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 del Consiglio dei Ministri 22 Febbraio 2013 (G. U. n.117 del 21 Maggio 2013). Referenziato nel seguito come DPCM.

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

[3] Decreto Legislativo 4 aprile 2006, n.159 (G.U. n.99 del 29 aprile 2006) - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.

[4] 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)

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

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

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

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

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

[10] Legge 24 Dicembre 1993, n. 537

[11] Legge 23 Dicembre 1993, n. 547

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

[13] Determinazione DigitPA n. 69/2010 - Modifiche alla Deliberazione CNIPA n. 45/2009

[14] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 19 luglio 2012 – Definizione dei termini di validità 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)

[eIDAS] REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE di seguito **eIDAS**

Riferimenti tecnici

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

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

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

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

[19] ETSI EN 319 401 V2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[20] ETSI EN 319 421 V1.1.1 -Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps di seguito **ETSI319421**

[21] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles di seguito **ETSI319422**

1.3 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal TU, dal CAD e dal DPCM 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.

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

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

Nel certificato compaiono altre informazioni tra cui:

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

Certificato Qualificato – cfr. CAD

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD

Certificatore Qualificato – cfr. CAD

Chiave Privata e Chiave Pubblica – cfr. CAD

Codice di emergenza (ERC)
Codice consegnato dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di sospensione di un certificato. Può essere preimbustato oppure in formato elettronico opportunamente protetto.

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. Può essere una smart card, un token USB oppure un HSM.

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

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

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

Giornale di controllo
Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [1].

Lista dei Certificati Revocati o Sospesi *[Certificate Revocation List]*
È 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 vedi validazione temporale

Manuale Operativo – cfr. art. 40 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 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.

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

Prestatore di servizio fiduciario – cfr eIDAS

Prestatore di servizi fiduciari qualificati – cfr eIDAS

RAO – Registration Authority Officer
Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un

Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.

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

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

Regole tecniche
Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici [1].

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]*
È 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.

Servizio fiduciario - cfr eIDAS

Servizio fiduciario qualificato- cfr eIDAS

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

Time-stamp policy
Insieme di regole che indicano l'applicabilità di una marca temporale in una particolare comunità con requisiti di sicurezza comune – cfr ETSI319421

Time-stamping service
Servizio fiduciario che emette marche temporali – cfr ETSI319421 [21]

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.

Validazione temporale elettronica
Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento [eIDAS]

Validazione temporale elettronica qualificata

una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 [eIDAS]

1.4 Acronimi e abbreviazioni

AgID – Agenzia per l'Italia Digitale

BTSP - Best practices Time-Stamp Policy [26]

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

CRL – Certificate Revocation List

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

DPCM - Decreto del Presidente del Consiglio dei Ministri
Ci si riferisce al DPCM 22 febbraio 2013.

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
È 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.

LUL – Libro Unico del Lavoro
Libro che sostituisce i libri paga e matricola e gli altri libri obbligatori dell'impresa: è stato istituito con gli articoli 39 e 40 del decreto-legge n. 112/2008 (convertito con legge 6 agosto 2008, n. 133).

OID – Object Identifier
È 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
Acronimo di Revocation Request Code, nome assegnato in precedenza al codice di emergenza e saltuariamente ancora utilizzato.

TSA – Time Stamping Authority
Prestatore di servizi fiduciari che utilizza uno o più sistemi di emissione di marca temporale – cfr ETSI319421

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

TSU – Time Stamp Unit
Insieme di hardware e software gestito come un unico sistema di marcatura temporale composto di una sola chiave attiva – cfr ETSI319421

TSP - Trust Service Provider
vd. Prestatore di servizi fiduciari

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"*.

UTC - Coordinated Universal Time
Tempo coordinato universale come definito in ITU-R TF.460-6 (2000)– cfr ETSI319421

2 Generalità

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

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

Questo documento evidenzia le regole generali e le procedure seguite dal **Certificatore Accreditato** Zucchetti (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 riportata 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 Zucchetti – Manuale Operativo" ed è caratterizzato dal codice documento: **ZUCCHETTI-MO**.
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.
Al documento sono associati tre **object identifier**, referenziati nell'estensione CertificatePolicy dei certificati secondo l'utilizzo cui gli stessi sono destinati.
Il significato degli OID e il seguente:

L'*object identifier* (OID) **1.3.76.45.1.1.1** identifica

Zucchetti	1.3.76.45
certification-service-provider	1.3.76.45.1
certificate-policy	1.3.76.45.1.1
manuale-operativo-firma-digitale	1.3.76.45.1.1.1

L'*object identifier* (OID) **1.3.76.45.1.1.2** identifica

Zucchetti	1.3.76.45
certification-service-provider	1.3.76.45.1
certificate-policy	1.3.76.45.1.1
Manuale-operativo-firma-automatica basata su HSM	1.3.76.45.1.1.2

L'*object identifier* (OID) **1.3.76.45.1.1.4** identifica

Zucchetti	1.3.76.45
certification-service-provider	1.3.76.45.1
certificate-policy	1.3.76.45.1.1
Manuale-operativo-firma-remota basata su HSM	1.3.76.45.1.1.4

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

- 1.3.76.45.1.1.1 → **OID1 –**
- 1.3.76.45.1.1.2 → **OID2 –**
- 1.3.76.45.1.1.4 → **OID3 –**

L'*object identifier* (OID) **1.3.76.45.1.1.3** identifica

Zucchetti	1.3.76.45
certification-service-provider	1.3.76.45.1
certificate-policy	1.3.76.45.1.1
Manuale operativo per il servizio fiduciario di validazione temporale qualificato a norma EIDAS	1.3.76.45.1.1.3

Questo documento è pubblicato in formato elettronico presso il sito Web del Certificatore all'indirizzo: http://www.firmadigitale.zucchetti.it

2.2 Attori e Domini applicativi

2.2.1 Certificatore

Zucchetti 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 [1] e secondo quanto prescritto dal **Codice dell'Amministrazione Digitale**.
I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Tabella 2-1

Denominazione Sociale	Zucchetti S.p.A. ad azionista unico
Sede legale	**Via Solferino, 1 - 26900 Lodi**
Rappresentante legale	Alessandro Zucchetti
N° telefono	**+39 03715941**
PEC	**zucchettispa@gruppozucchetti.it**
N° iscrizione Registro Imprese	**Lodi, n° 05006900962**
N° partita IVA	**05006900962**
Sito web	**www.zucchetti.it**

2.2.2 Uffici di Registrazione

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

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

Possono svolgere il ruolo di Uffici di Registrazione anche altri soggetti che stipulino con il

Certificatore un'apposita convenzione.
L'Ufficio di Registrazione, anche tramite suoi incaricati, svolge in sostanza tutte le attività di interfaccia tra il Certificatore ed il Richiedente della 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 o presso il Titolare.
Il Certificatore verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo Manuale.

2.2.3 Registro dei Certificati

Le liste di revoca e di sospensione dei certificati sono pubblicate in un registro pubblico che contiene anche i certificati dei titolari che ne hanno fatto espressa richiesta.
Il registro dei certificati, che contiene tutti i certificati emessi dal Certificatore, **non** è pubblico.
Il Certificatore utilizza sistemi affidabili per la gestione del registro pubblico e del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza.

2.2.4 Applicabilità

I certificati emessi dal Certificatore Accreditato **Zucchetti** 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 **Zucchetti** 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.

2.3 Contatto per utenti finali e comunicazioni

Zucchetti 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:

Zucchetti
Responsabile della Certification Authority
Via Solferino, 1
26900 Lodi

Web: www.firmadigitale.zucchetti.it
e-mail: assistenza.certifica@zucchetti.it

I riferimenti del Call Center Firma Digitale sono riportati nel sito web della Certification Authority www.firmadigitale.zucchetti.it.

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

2.4 Rapporti con l'Autorità di Vigilanza

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 da AgID al fine dello scambio delle informazioni attraverso un sistema sicuro di comunicazione.

Il certificato emesso ai sensi dell'articolo 39 del decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 129, del 6 giugno 2009, relativo alle chiavi con cui viene firmato l'elenco pubblico dei certificatori accreditati è caratterizzato dall'OID 1.3.76.45.1.1.26

3 Regole Generali

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

3.1 Obblighi e Responsabilità

3.1.1 Obblighi del Certificatore

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

1. siano soddisfatte tutte le regole tecniche specificate nel DPCM [1];
2. siano soddisfatte le modalità di riconoscimento del Titolare ai sensi delle norme [2], con particolare riguardo all'identificazione certa del Titolare;
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'elenco dei certificatori, 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. 32, comma 3, lett. b) del CAD;
7. i Titolari siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi nonché riguardo agli obblighi da essi assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi sicuri di firma;
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, del Terzo Interessato o del Richiedente, di compromissione della chiave privata, di provvedimento dell'autorità, d'acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti di abusi o falsificazioni;
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. **OID1 -** non si rende depositario di dati per la creazione della firma del Titolare;
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. **OID1 -** al momento del rilascio del certificato il Titolare detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato
18. **OID2/OID3 -** i dati per la creazione della firma siano sotto il controllo esclusivo del Titolare.

3.1.2 Obblighi dell'Ufficio di Registrazione

L'Ufficio di Registrazione è tenuto a garantire:

1. che il Titolare sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito

alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma;
2. che il Titolare sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. 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. la verifica d'identità del Titolare del certificato, il controllo e la registrazione dei dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;
5. 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;
6. la comunicazione al Certificatore di tutti i dati e documenti acquisiti durante l'identificazione allo scopo di attivare la procedura di emissione del certificato;
7. la verifica e inoltro al Certificatore delle richieste di revoca, sospensione e rinnovo attivate dal Titolare presso l'Ufficio di Registrazione;
8. l'esecuzione, ove prevista a suo carico dal presente Manuale Operativo, della revoca o sospensione dei certificati;
9. l'invio tempestivo al Certificatore degli originali delle richieste di certificazione;
10. 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 il Richiedente e con i Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Manuale Operativo.

3.1.3 Obblighi dei Titolari

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

3.1.4 Obblighi degli Utenti

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

3.1.5 Obblighi del Terzo Interessato

Il Terzo Interessato, che, **avendo presa visione del presente Manuale Operativo**, manifesta il proprio consenso all'inserimento nel certificato di un Ruolo oppure autorizza o richiede l'indicazione dell'Organizzazione a cui il Titolare è collegato, è tenuto a:
1. attenersi a quanto disposto dal presente Manuale Operativo;
2. provvedere tempestivamente all'inoltro, con le modalità descritte ai paragrafi § 5.4.2 e § 5.4.5, della richiesta di revoca o sospensione nei casi previsti ai paragrafi § 5.4.1 e § 5.4.4.

3.1.6 Obblighi del Richiedente

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

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, § 3.1.5 e § 3.1.5 costituisce inadempimento essenziale ai sensi dell'art. 1456 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 si assume le responsabilità previste dal CAD, per i soggetti che svolgono funzione di Certificatore.

3.4 Pubblicazione

3.4.1 Pubblicazione di informazioni relative al Certificatore

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web del Certificatore (cfr. § 2.1)
- in formato cartaceo, richiedibile sia al Certificatore sia al proprio Ufficio di Registrazione.

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative al Certificatore previste dal DPCM sono pubblicate presso l'elenco 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.firmadigitale.zucchetti.it) firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione, via e-mail all'indirizzo richiesta.pubblicazione@zucchetti.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 protocolli LDAP ed HTTP. L'indirizzo (URL) ldap ed http è indicato nell'apposita estensione del certificato denominata "Punti di distribuzione Elenco dei certificati revocati" (in inglese: CRL distribution point).
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 i protocolli LDAP ed HTTP.
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 indicate sul sito web all'indirizzo: www.firmadigitale.zucchetti.it

3.7.2 Accesso al certificato e alle liste di revoca

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

4 Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per:

- l'identificazione del Titolare al momento della richiesta di rilascio del certificato qualificato di sottoscrizione;
- l'autenticazione del Titolare nel caso di rinnovo, revoca e sospensione del certificato qualificato di sottoscrizione;
- l'autenticazione dell'eventuale Terzo Interessato, in caso di sua richiesta di revoca o sospensione del certificato qualificato del Titolare.

4.1 Identificazione ai fini del primo rilascio

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

La modalità di identificazione comporta che il Titolare sia riconosciuto personalmente da uno dei soggetti di cui al § 4.1.1, che ne verificherà l'identità attraverso il controllo della carta d'identità o di un documento ad essa equipollente (cfr. art. 35 comma 2 del TU) in corso di validità, salvo ulteriori restrizioni indicate nel seguito.

Il Certificatore verifica inoltre la documentazione comprovante il Ruolo.

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 (cfr. Allegato B).

Modalità 2

1. Identificazione tramite firma digitale.

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 1

L'identificazione è effettuata da uno dei soggetti indicati al § 4.1.1 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 [4]:

- Carta d'identità
- Passaporto
- Patente di guida

Il codice di emergenza costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro

tra Certificatore e Titolare (cfr. art. 21 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.

4.1.2.2 Riconoscimento effettuato secondo la modalità 2

Nella modalità 2 il Certificatore si basa sul riconoscimento già effettuato da un altro Certificatore. Il Titolare è già in possesso di un dispositivo di firma con un certificato qualificato a bordo ancora in corso di validità. Il riconoscimento avviene in maniera analoga a quanto previsto dalla procedura di rinnovo (§4.2).
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

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

Si riportano di seguito i passi principali a cui il Titolare deve attenersi per ottenere un certificato di sottoscrizione:

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 capitolo;
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.

4.1.3 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. Il modulo di richiesta deve essere sottoscritto dal 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, quali tipo, numero, ente emittente e data di rilascio dello stesso
- Indirizzo e-mail per l'invio delle comunicazioni dal Certificatore al Titolare.
- **OID2/OID3 -** numero di telefonia mobile per la trasmissione della OTP ove fosse questa la tecnologia OTP adottata

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

[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

4.1.4 Uso di pseudonimi

I certificati emessi da Zucchetti non prevedono l'uso dello pseudonimo.

4.1.5 Limiti di valore e limiti d'uso

E' facoltà del Titolare richiedere al Certificatore l'inserimento nel certificato di limiti di valore che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. I valori devono essere espressi come numeri interi positivi, senza indicazione di cifre decimali.
Per quanto riguarda i limiti d'uso, allo stato attuale, Zucchetti ha predisposto questa indicazione per i certificati relativi a chiavi adoperate per l'apposizione di firme automatiche che contengono la seguente limitazione d'uso:
Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended automatic digital signature.

Zucchetti rilascia anche certificati con le seguenti limitazioni 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.
- The certificate holder must use the certificate only for signing electronic documents of the Organization indicated in the certificate Organization field.
- Il certificato è valido solo per la firma automatica di: LUL, fatture, atti per previdenza, assistenza e tributi, privacy, sicurezza lavoro, ricorsi, documenti informatici, deleghe per atti predetti.
- This certificate is valid only for signatures on documents of kind single work ledger, bills, acts related to tributes and social security, for creation of e-documents and copies in the mentioned.

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 gestita di conseguenza.
Oltre ai limiti suddetti, il Certificatore adotta i limiti d'uso pubblicati sul sito dell'Autorità di Vigilanza.

4.1.6 Inserimento del Ruolo e dell'Organizzazione nel certificato

Il Titolare può ottenere, direttamente, o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di sottoscrizione di informazioni relative a Funzioni, Titoli e/o Abilitazioni Professionali e Poteri di Rappresentanza.
In questo caso, il Titolare, oltre alla documentazione e alle informazioni identificative necessarie (cfr. §4.1.3, §4.1.4, §4.1.5), dovrà produrre anche quella idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo, ove espressamente consentito dal presente Manuale Operativo, mediante Autocertificazione, ai sensi dell'art. 46 del D.P.R. 445/2000.
Come indicato nella Deliberazione CNIPA [4], nel caso in cui la richiesta di inserimento del ruolo nel certificato sia stata effettuata mediante la sola autocertificazione da parte del Titolare, il certificato non riporterà informazioni inerenti l'organizzazione a cui potrebbe eventualmente essere legato il ruolo stesso.
Il Certificatore, in tali ipotesi, non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, in merito all'inserimento nel certificato delle informazioni autocertificate dal Titolare.
La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se essa ha autorizzato (Terzo Interessato) il rilascio del certificato al Titolare, anche senza l'esplicita indicazione di un ruolo.
In tale ipotesi il Certificatore effettua un controllo sulla regolarità formale della documentazione presentata dal Titolare.

La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni in possesso di Codice Fiscale.
Le informazioni inerenti al Ruolo che possono essere inserite nel certificato rientrano nelle seguenti categorie:

- Titoli e/o abilitazioni Professionali;
- Poteri di Rappresentanza di 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.

Il certificato, per quanto riguarda la modalità con cui viene attestato il Ruolo del titolare, è conforme a quanto indicato nella Deliberazione CNIPA [5] e nel documento "Linee Guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei Titolari dei certificati elettronici" (OID=1.3.76.24.1.1.1) emesso da AssoCertificatori e disponibile sul sito http://www.assocertificatori.org.

4.1.6.1 Titoli e/o Abilitazioni Professionali

Nel caso in cui sia richiesta l'indicazione nel certificato di Abilitazioni Professionali per l'esercizio delle quali sia necessario ottenere preventivamente l'iscrizione all'Albo su verifica dell'Ordine professionale competente alla tenuta e vigilanza dello stesso, il Titolare, salvo diversa pattuizione tra il Certificatore e l'Ordine di appartenenza, dovrà fornire un certificato rilasciato dall'Ordine, o un'autocertificazione ai sensi dell'art. 46 del D.P.R. n. 445/2000, ed il consenso scritto da parte di quest'ultimo manifestato sull'apposito modulo fornito dal Certificatore.

La documentazione da presentare ai sensi dei commi precedenti non dovrà essere anteriore di oltre 10 (dieci) giorni alla data della richiesta di registrazione.

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

Per l'esercizio delle professioni per le quali sia richiesto l'iscrizione ad 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.

4.1.6.2 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.

4.1.6.3 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 [14].

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 al 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, 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 colui che effettua la richiesta di revoca o di sospensione.

4.3.1 Richiesta da parte del Titolare

Se la richiesta viene effettuata per telefono oppure 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 tramite 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 §5.4.2.
Il Certificatore si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del Terzo Interessato in apposite convenzioni da stipulare con lo stesso.

4.3.3 Richiesta da parte del Richiedente

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

5 Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore.
La registrazione iniziale è effettuata presso il Certificatore oppure presso un Ufficio di Registrazione anche telematicamente.

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

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

OID1 - La seconda modalità (nel seguito Caso B) prevede una separazione tra la fase di identificazione, effettuata in presenza del Titolare, e quella di registrazione ed emissione del certificato, che viene effettuata successivamente dai RAO. L'SSCD (smart card o token USB) viene personalizzato a cura del Certificatore con il PIN consegnato al Titolare al momento dell'identificazione. L'SSCD è consegnato al Titolare in un secondo momento.

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

OID1/OID2/OID3 - La quarta modalità (nel seguito Caso D) si applica ai rilasci telematici con Busta ERC virtuale. Ed include la possibilità che il Titolare già sia in possesso di un dispositivo di firma.

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

5.2 Rilascio del certificato

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

Questa procedura prevede la presenza del Titolare cui viene contestualmente consegnato il dispositivo a microprocessore presso un Ufficio di Registrazione o presso il Certificatore.

1. Il RAO, contestualmente all'identificazione, registra il Titolare e attiva la procedura di rilascio di certificato.
2. La procedura automatica sblocca il dispositivo sicuro di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia e la predisposizione della richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della smartcard (PKCS#10). Nel caso in cui il dispositivo sicuro di firma abbia un PIN differente da quello di default, la procedura richiede l'inserimento del PIN da parte del Titolare.
3. Il RAO, utilizzando il proprio dispositivo, firma il PKCS#10 imbustandolo in un PKCS#7 e la invia al Certificatore.

4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo sicuro di firma inserendo il PIN già consegnato al Titolare in fase di identificazione

5.2.2 OID1 - Caso B: Chiavi generate dal Certificatore

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

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

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

5.2.3 OID2 - Caso C: Chiavi generate in dispositivi HSM (Firma automatica)

Questa procedura viene effettuata da personale del Certificatore o da procedure automatiche presso i locali che ospitano l'HSM ed i server collegati. Il certificato emesso è inviato al Titolare. Certificato e chiavi sono resi "non funzionali" fino a che il Titolare stesso non provveda a richiederne l'attivazione.
Le modalità di registrazione del Titolare e di rilascio della Busta ERC possono seguire quanto descritto nei casi B o D, secondo l'organizzazione dell'Ufficio di Registrazione ed i rapporti che questo ha stabilito con il Certificatore.

5.2.4 OID1/OID2/OID3 - Caso D: Rilascio Telematico

Il Titolare si collega al sito del Certificatore e compila il form di registrazione.

Se già in possesso di firma digitale:

- visualizza e controlla il contratto precompilato attraverso il form
- sottoscrive il modulo con la sua firma digitale
- invia il modulo a Zucchetti mediante le funzionalità disponibili sul sito del Certificatore

Se non in possesso di firma digitale:

- scarica il modulo precompilato e lo firma
- fa autenticare la firma autografa del modulo da parte di un Pubblico Ufficiale
- invia il modulo a Zucchetti in originale con copia documenti necessari all'identificazione validi non scaduti

Zucchetti, verificata la correttezza dei dati ricevuti, invia all'indirizzo email specificato nel modulo di registrazione i codici ERC, crittografati con la passphrase che il Titolare stesso ha definito nel modulo.
Qualora si tratti di token o smart card, la procedura genera, analogamente a quanto previsto nel caso B,

la nuova coppia di chiavi sul dispositivo del Titolare, che viene poi inviato all'indirizzo dichiarato all'atto della registrazione.
Qualora si tratti di Firma Remota, all'utente vengono inviate le istruzioni e le credenziali per la generazione autonoma della coppia di chiavi.
L'invio telematico della busta ERC può avvenire anche nei casi di contratto cartaceo con identificazione del Titolare tramite le modalità descritte nel paragrafo § 4.1.

5.2.5 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 minima delle chiavi è di 2048 bits.

5.2.6 Protezione delle chiavi private

OID1 - La chiave privata del Titolare è generata e memorizzata in un'area protetta della carta a microprocessore che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.
OID2/OID3 - La chiave privata del Titolare è generata e memorizzata in un'area protetta del dispositivo HSM che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione cancella la propria memoria, a protezione dei dati in essa contenuti.

5.3 Emissione del certificato

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

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

   OID2/OID3 - il certificato viene memorizzato nei server del Certificatore e ne viene data comunicazione al Titolare

7) Si distinguono i casi:
   - **OID1 –** (Caso A) il Titolare è già in possesso del dispositivo sicuro di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione;
   - **OID1 -** (Caso B): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato a cura dell'Ufficio di Registrazione al Titolare;

- **OID2 -** (Caso C): il Titolare è già in possesso del dispositivo/credenziali per l'attivazione della firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione;
- **OID1/OID2/OID3 -** (Caso D): il Titolare è già in possesso del dispositivo/credenziali per l'attivazione della firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.

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

5.3.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni relative al Titolare ed indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme a quanto specificato nella Deliberazione CNIPA [5]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.
Il certificato contiene un'apposita estensione [Qualified Certificate Statements - esi4-qcStatement-1 (OID: 0.4.0.1862.1.1)] la quale indica che il certificato è qualificato.

5.3.2 Pubblicazione del certificato

Al buon esito della procedura di certificazione il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico. 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 è determinato sulla base:

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

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

5.4 Revoca e sospensione di un certificato

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

5.4.1 Motivi per la revoca di un certificato

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

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
   - sia stato smarrito il dispositivo sicuro di firma che contiene la chiave;

- sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN);
- si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;

2. il Titolare non riesce più ad utilizzare il dispositivo sicuro di firma in suo possesso (es. guasto del dispositivo);
3. si verifica un cambiamento dei dati del Titolare presenti nel certificato, ivi compresi quelli relativi al Ruolo, tale da rendere detti dati non più corretti e/o veritieri;
4. viene a mancare l'associazione tra il Titolare e l'Ordine che ne ha convalidato l'affiliazione;
5. termina il rapporto tra il Titolare e il Certificatore;
6. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

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

5.4.2 Procedura per la richiesta di revoca

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

5.4.2.1 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 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.

5.4.2.2 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.

5.4.2.3 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.

5.4.2.4 Revoca su iniziativa del Richiedente

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

1. il Richiedente richiede per iscritto al Certificatore la revoca del certificato compilando l'apposito modulo messo a disposizione dal Certificatore stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del Titolare del certificato comunicati dal Certificatore al momento dell'emissione del certificato. Il Richiedente è tenuto ad autenticarsi secondo quanto previsto al paragrafo § 3.;
2. Il Certificatore, verificata l'autenticità della richiesta, la comunica al Titolare, secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla revoca del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

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

5.4.3 Procedura per la revoca immediata

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

5.4.5 Procedura per la richiesta di Sospensione

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

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

Sono previsti i seguenti casi:

5.4.5.1 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;
   - la data di fine sospensione;
   - il codice di emergenza;
2. telefonando al Call Center del Certificatore e fornendo le informazioni di cui al punto precedente. In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una sospensione immediata del certificato per una durata di 10 (dieci) giorni solari in attesa della richiesta scritta del Titolare; qualora il Certificatore, direttamente o tramite un Ufficio di Registrazione, non riceva la richiesta sottoscritta entro il termine indicato, il certificato verrà riattivato.
3. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione al Certificatore.

Il Titolare è tenuto a sottoscrivere la richiesta di sospensione e consegnarla all'Ufficio di Registrazione o inviarla direttamente al Certificatore per lettera, per fax o tramite pec 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.

5.4.5.2 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 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.

5.4.5.3 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 per iscritto al Certificatore la sospensione 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, la decorrenza e la data di termine della sospensione. Il Terzo Interessato è tenuto ad autenticarsi secondo quanto previsto al paragrafo § 4.3.2.;
2. il Certificatore, verificata l'autenticità della richiesta, la comunica al Titolare secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato inserendolo nella lista di revoca e sospensione (CRL).

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

5.4.5.4 Sospensione su iniziativa del Richiedente

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

1. il Richiedente richiede per iscritto al Certificatore la sospensione 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, la decorrenza e la data di termine della sospensione. Il Richiedente è tenuto ad autenticarsi secondo quanto previsto al paragrafo §4.3.3;
2. il Certificatore, verificata l'autenticità della richiesta, la comunica al Titolare secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato inserendolo nella lista di revoca e sospensione (CRL).

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

5.4.6 Ripristino di validità di un Certificato sospeso

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

Qualora la scadenza della sospensione coincida con la scadenza del certificato o sia a questa successiva, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

5.4.7 Pubblicazione e frequenza di emissione della CRL

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

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

5.4.8 Tempistica

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di 24 ore.
In caso di revoca o sospensione immediata il tempo di attesa è al massimo di 4 ore.

5.5 Sostituzione delle chiavi e rinnovo del Certificato

La procedura di richiesta di un nuovo certificato, che prevede la generazione di una nuova coppia di chiavi, deve essere avviata da parte del Titolare prima della scadenza del certificato (Cfr. §4.2) già in suo possesso.
La procedura di rinnovo si applica esclusivamente a certificati emessi dal Certificatore Zucchetti.
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 dalla sua scadenza.
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

Sul sito www.firmadigitale.zucchetti.it è gratuitamente scaricabile un prodotto (denominato "FirmaCheck") per consentire:

- di firmare digitalmente documenti a tutti i titolari in possesso di una smart card o token rilasciati da Zucchetti.
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Deliberazione CNIPA [13]
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Circolare AIPA 24/2000 [12].

Gli ambienti in cui FirmaCheck opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo: http://www.firmadigitale.zucchetti.it

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 FirmaCheck", facente parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.

OID3: L'apposizione di firma digitale si configura come un servizio on line, accessibile via rete (internet). La coppia delle chiavi crittografiche e il certificato digitale risiedono in modalità sicura nel SSCD (HMS) sito presso il Certificatore e accessibile da remoto con modalità sicure. Il Titolare viene identificato dal servizio ed autorizza l'apposizione della firma tramite un meccanismo di sicurezza: all'atto della firma del documento il Titolare utilizza una One Time Password (OTP) ricevuta in tempo reale sul dispositivo OTP e di un PIN di firma assegnato in fase del rilascio del certificato, noto a lui solo.
Il codice OTP è di fatto una password "usa e getta" di 6 cifre, integralmente inserite dal firmatario nell'apposito box di firma del documento; il codice PIN è composto da 8 cifre, inserite dal firmatario nel medesimo box di firma.

Il prodotto FirmaCheck 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

NOTA BENE. Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD. E' cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile. In Allegato C sono riportate le modalità operative, in riferimento ad alcuni formati, per accertarsi che il documento non contenga macroistruzioni o codici eseguibili.
Una nota particolare meritano i file con estensione HTM o HTML. Questi file sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Questi file, visualizzabili tramite

qualsiasi Web Browser, possono contenere sia 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 fiduciario qualificato di Validazione Temporale (1.3.76.45.1.1.3)

Zucchetti è prestatore di servizi fiduciari qualificati (Qualified trust service provider) per il servizio di validazione temporale. Il servizio soddisfa i requisiti di cui all'articolo 42 del regolamento eIDAS.

Questo capitolo è identificato dall'OID 1.3.76.45.1.1.3 definito nel paragrafo 2.1

Il servizio fornito da Zucchetti è conforme alla policy BTSP come definita in ETSI319421 [26] identificata dall'OID,

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)	0.4.0.2023.1.1

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

In generale, il servizio di marcatura temporale consente di stabilire l'esistenza di un documento informatico prima di un certo istante temporale associando all'evidenza informatica una data e ora certe validandola temporalmente.
Un'evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale ad essa associata: la marca temporale è una struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora).

La marca temporale viene firmata ed emessa da un prestatore di servizi fiduciari che fornisce sistemi di marcatura temporale (Time Stamping Authority (TSA)) che certifica le chiavi di un sistema fidato (Time Stamp Unit (TSU)) al quale gli utenti indirizzano le loro richieste secondo necessità; chiunque abbia richiesto e conservato una marca temporale per un certo documento potrà, in seguito, dimostrare che tale documento effettivamente esisteva alla data/ora riportate nella marca firmata da quella catena di certificazione TSU/TSA.
In particolare, la validazione temporale di un documento firmato digitalmente consente di verificare e considerare valida la firma digitale apposta anche quando il certificato del sottoscrittore risulti scaduto o revocato, purché l'assegnazione della marca temporale al documento sia stata effettuata durante il periodo di validità del certificato medesimo.

7.1 Richiesta di emissione o di verifica di marca temporale

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

La richiesta di emissione/verifica marca temporale può essere effettuata utilizzando il software di firma/verifica fornito da Zucchetti, che consente di apporre la marca temporale a documenti firmati digitalmente e di eseguirne un'immediata verifica.

Una volta accettata e registrata la richiesta ed effettuati gli opportuni controlli di correttezza, il server TSU la elabora, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della verifica opportunamente predisposto per la visualizzazione.

7.2 Emissione o verifica di marca temporale

L'emissione della marca temporale viene effettuata in modo automatico da un sistema elettronico sicuro (server TSU), gestito dalla TSA, in grado di:

- calcolare con precisione la data e ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato (UTC);
- generare la struttura di dati contenente le informazioni specificate nel successivo paragrafo 7.4.1;
- sottoscrivere digitalmente (nel significato tecnico del termine) detta struttura di dati.

L'operazione avviene secondo le fasi seguenti:

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

L'algoritmo utilizzato per l'impronta è SHA-256 (*secure hash algoritm 256-bit*)

7.3 Ciclo di vita delle chiavi e dei certificati di marcatura

La marca temporale viene firmata con algoritmo asimmetrico da una chiave privata memorizzata su un dispositivo hardware sicuro e la corrispondente chiave pubblica certificata da una certification authority dedicata a questo servizio.

7.3.1 Generazione della chiave di marcatura temporale della TSU

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware conforme ai requisiti di sicurezza previsti da ETSI319421 [20]. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 2048 bit.

7.3.2 Protezione della chiave privata della TSU

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

7.3.3 Ciclo di vita della chiave di marcatura della TSU

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata al sistema che fornisce il servizio. Le chiavi di marcatura temporale (chiavi TSU) vengono sostituite ogni sei mesi prima della scadenza del certificato senza revocare il precedente.

7.4 Distribuzione della chiave pubblica per la verifica della marca temporale

È garantita l'integrità e l'autenticità della chiave pubblica del server TSU in quanto distribuita tramite emissione di un certificato di chiave pubblica sottoscritto dal prestatore di servizi qualificati Zucchetti S.p.A..
L'emissione del certificato per la verifica delle marche emesse viene effettuato in modo automatico dalle procedure della TSA secondo i seguenti passi:

- viene generata la richiesta di certificato da parte del personale autorizzato e inoltrata alla CA Zucchetti dedicata alla certificazione di chiavi di marcatura temporale (TSA);
- si procede alla generazione del certificato;
- il certificato viene inviato ad AGID che lo rende disponibile attraverso l'elenco dei prestatori di servizi fiduciari in Italia. A livello europeo la lista viene pubblicata insieme a quelle degli altri stati.

Il formato del certificato di marcatura temporale, contenente la chiave pubblica della TSU, è conforme a quanto specificato in ETSI319422[21]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa eIDAS e italiana.

7.4.1 Conservazione della marca temporale

Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a 20 (venti) anni.

7.5 Marca Temporale

7.5.1 Formato e contenuto della marca temporale

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche richieste in ETSI319422 [21].
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. (sha256WithRSAEncryption OID:1.2.840.113549.1.1.11)
- l'identificativo del certificato relativo alla chiave pubblica della TSU.
- la data e l'ora di generazione della marca.
- l'accuracy della fonte del tempo rispetto ad UTC. Nella fattispecie è di un secondo o migliore.
- l'identificativo dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale. Nella fattispecie l'algoritmo utilizzato è SHA-256 (s*ecure hash algoritm 256-bit OID:2.16.840.1.101.3.4.2.1*)
- il valore dell'impronta dell'evidenza informatica.

7.5.2 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 dispositivi crittografici personali.

Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione.

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

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

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

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

8 Controllo del sistema di certificazione

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

8.1 Strumenti automatici per il controllo di sistema

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

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

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

8.2 Verifiche di sicurezza e qualità

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

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

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

Le registrazioni di questi eventi costituiscono il giornale di controllo.

9 Dati archiviati

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

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

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

9.1 Procedure di salvataggio dei dati

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

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

10 Sostituzione delle chiavi del Certificatore

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

11 Cessazione del servizio

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

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

12 Sistema di qualità

Zucchetti ha ottenuto la certificazione ISO 9001 il 12 dicembre 2000, quella ISO 27001 il 17 agosto 2011.

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	Tramite modalità web: Dalle 0:00 alle 24:00 7 giorni su 7 Altre modalità: dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi
Altre attività: registrazione, generazione, pubblicazione, rinnovo (*)	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi
Richiesta e/o verifica di marca temporale	24hx7gg (disponibilità minima 95%)

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

14 Misure di Sicurezza

Il sistema di sicurezza del servizio di certificazione digitale 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 all'Autorità di Vigilanza entro 24 ore;
c) informare tutte i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata;
d) revocare tutti i certificati qualificati sottoscritti con la chiave compromessa;
e) nel caso di revoca del punto precedente saranno riemessi i certificati delle chiavi pubbliche dei titolari utilizzando una nuova chiave di certificazione.

14.3 Procedure di Gestione dei Disastri

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

15 Amministrazione del Manuale Operativo

15.1 Procedure per l'aggiornamento

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

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

Ogni anno il Certificatore comunica ad AgID 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.

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

15.2 Regole per la pubblicazione e la notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del Certificatore (indirizzo: http://www.firmadigitale.zucchetti.it);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto dall'Autorità di Vigilanza;
- in formato cartaceo può essere richiesto agli Uffici di Registrazione.

15.3 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Presidente del Consiglio di Amministrazione e Rappresentante legale di Zucchetti – Autorità di Certificazione.

15.4 Conformità

I contenuti del presente Manuale Operativo sono pienamente rispondenti alle regole tecniche descritte nel DCPM [1].

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 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

16.3.1 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.

16.3.2 Lunghezza delle chiavi

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

16.3.3 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.

16.3.4 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.

16.3.5 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.

16.3.6 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.

16.3.7 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 Modalità operative in caso di Identificazione da parte di Pubblici Ufficiali in Italia

Il Titolare può compilare la richiesta di Certificazione (disponibile sul sito www.firmadigitale.zucchetti.it) e sottoscriverla, facendo autenticare la propria firma autografa, ai sensi delle normative vigenti, da un Pubblico Ufficiale.

La richiesta di certificazione, completa di tutti i dati previsti (§4.1.2.1) così sottoscritta può essere inviata:

- al Certificatore agli indirizzi di riferimento (§2.3),
- ad uno degli Uffici di Registrazione all'uopo autorizzati reperibili sul sito www.firmadigitale.zucchetti.it

con l'indicazione dell'indirizzo cui dovrà essere spedito il dispositivo di firma. Le credenziali verranno inviate per email all'indirizzo indicato dal Richiedente nel modulo di registrazione, crittografate con la passphrase che il Richiedente ha indicato nel modulo stesso.

17.2 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 2007, MS Excel 2007 e Acrobat Reader XI, tutte nelle relative versioni in lingua italiana.
Le estensioni dei file associate dal sistema operativo Windows a queste applicazioni sono comunemente le seguenti: .docx, .xlsx, .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 C.1 MS Word e MS Excel

18.1.1 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 si possono seguire i seguenti passi:

1. Fare clic sul pulsante **Microsoft Office**, scegliere **Opzioni di Excel/Word**, **Centro Protezione**, **Impostazioni centro protezione**, quindi **Impostazioni Macro**
2. Selezionare l'opzione desiderata. L'opzione **Disattiva tutte le macro senza notifica** disattiva automaticamente tutte le macro. L'opzione **Disattiva tutte le macro tranne quelle con firma digitale** consente l'apertura automatica (ovvero l'esecuzione) delle sole macro firmate digitalmente da editori attendibili[2]. Le macro non firmate verranno disattivate automaticamente. L'opzione **Disattiva tutte le macro con notifica** disattiva automaticamente tutte le macro ma invia avvisi di protezione se vengono rilevate. In questo modo, è possibile scegliere se attivare le macro caso per caso.

Si noti che pur essendo disattivate le macro continuano ad essere presenti nel documento, pertanto sottoscrivendo il documento con firma digitale, si sottoscrivono anche le eventuali macro. Per tale ragione si consiglia di scegliere l'opzione **Disattiva tutte le macro con notifica** in modo da avere evidenza della presenza delle stesse.

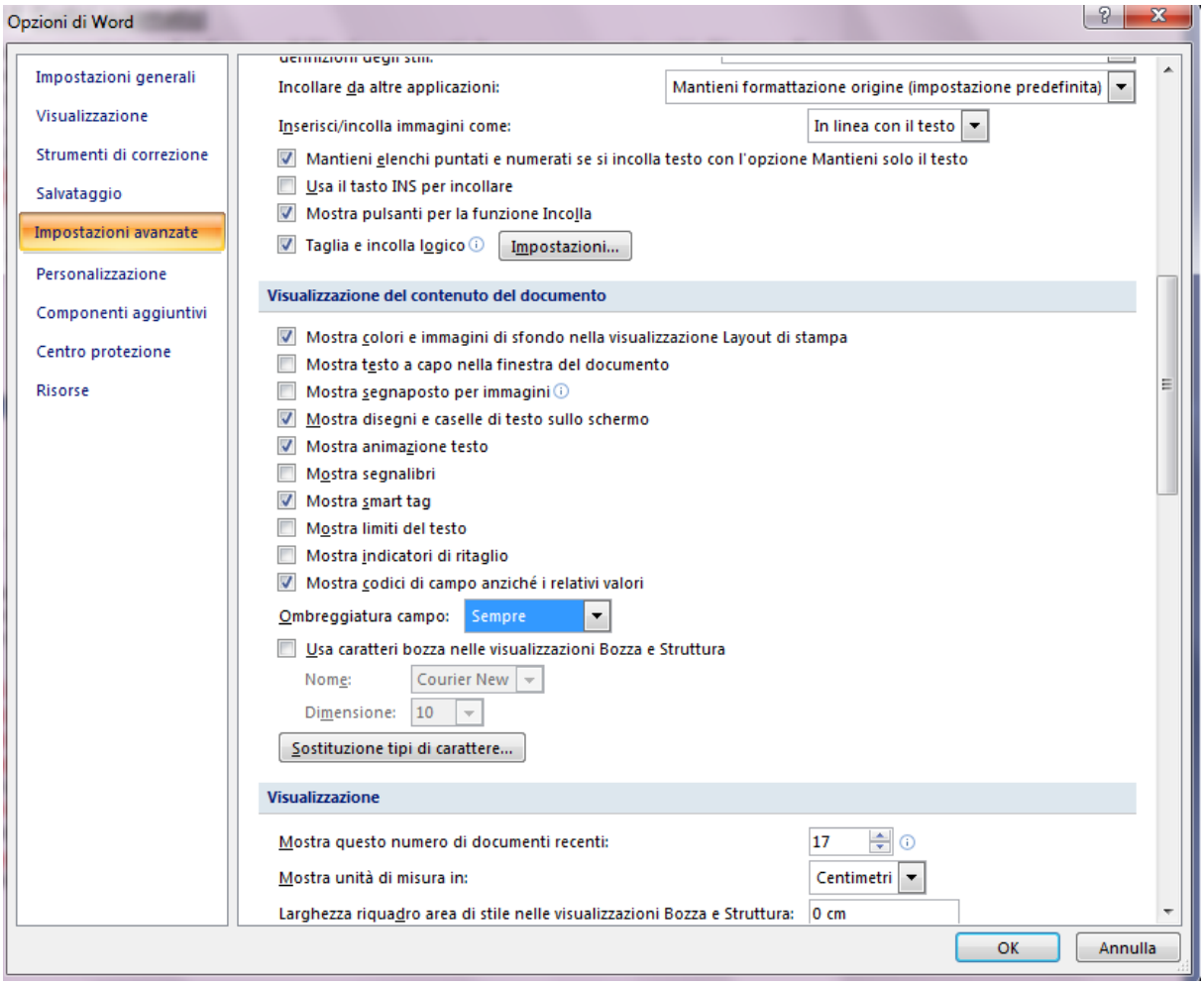
Per una panoramica completa del comportamento di MS Word e MS Excel in presenza di macro, consultare le Guide in linea dei prodotti.

18.1.2 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:

[2] L'elenco degli editori attendibili può essere consultato ed aggiornato selezionando il pulsante **Microsoft Office**, **Opzioni di Excel/Word, Centro Protezione**, quindi **Impostazioni centro Protezione** e **Editori attendibili**.

1. Fare clic sul pulsante **Microsoft Office**, scegliere **Opzioni di Word**, quindi **Impostazioni Avanzate**, sezione **Visualizzazione del contenuto del documento**.
2. Attivare lw check box **Mostra disegni e caselle di testo sullo schermo** e **Mostra i codici di campo** anziché i relativi valori per visualizzare.
3. Selezionare dal sottostante menu **Ombreggiatura campo**: **Sempre**



18.1.3 Formule

Per visualizzare tutte le formule sul foglio di lavoro si sceglie **Formule**, **Verifica Formule** si seleziona **Mostra Formule**. Per nasconderle si esegue la stessa procedura e si deseleziona **Mostra** Formule.

18.2 C.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.