Zucchetti

Autorità di Certificazione

Certificati di Sottoscrizione
Manuale Operativo

ZUCCHETTI-MO

Questa pagina è lasciata
intenzionalmente bianca

Indice

1 INTRODUZIONE

1.1 Quadro Generale

Un certificato lega la chiave pubblica ad un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata: tale persona fisica è il **Titolare** del certificato. Il certificato è usato da altre persone per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma elettronica qualificata apposta o associata ad un documento. Il certificato garantisce la corrispondenza tra la chiave pubblica ed il Titolare. Il grado d'affidabilità di quest'associazione è legato a diversi fattori: la modalità con cui la Certification Authority ha emesso il certificato, le misure di sicurezza adottate, gli obblighi assunti dal Soggetto per la protezione della propria chiave privata, le garanzie offerte.

Il presente documento è il Manuale Operativo, del **Prestatore di Servizi Fiduciari Zucchetti** (*Trust Service Provider*).
Il manuale contiene le politiche e le pratiche seguite nel processo di identificazione e emissione del certificato qualificato, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, e in generale di tutto ciò che rende affidabile un certificato qualificato in conformità con la vigente normativa.
Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nei certificati, si consente agli utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione e quindi del legame tra chiave e Titolare.
Il contenuto si basa sulle norme vigenti alla data di emissione e recepisce le raccomandazioni del documento "Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003.

1.2 Nome e identificativo del documento

Questo documento è denominato "Certificati di Sottoscrizione – 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 gli **object identifier**, descritti di seguito, che sono 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) che identifica Zucchetti è 1.36.76.45

Le policy per certificati qualificati su dispositivo qualificato sono:

Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo qualificato (QSCD)	**1.3.76.45.1.1.1** policy 0.4.0.194112.1.2	conforme alla QCP-n-qscd
Manuale-operativo-certificato qualificato emesso a persona fisica per firma automatica remota su dispositivo (QSCD)	**1.3.76.45.1.1.2** policy 0.4.0.194112.1.2	conforme alla QCP-n-qscd
Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo (QSCD)	**1.3.76.45.1.1.4** policy 0.4.0.194112.1.2	conforme alla QCP-n-qscd

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

1.3 Partecipanti e responsabilità

1.3.1 Certification Authority – Autorità di Certificazione

La **Certification Authority** è il soggetto terzo e fidato che emette i certificati qualificati di firma digitale, firmandoli con la propria chiave privata, detta chiave di CA o chiave di root.
Zucchetti è la Certification Authority (**CA**) che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle regole tecniche emanate dall'Autorità di Vigilanza e secondo quanto prescritto dal Regolamento eIDAS [1] e dal Codice dell'Amministrazione Digitale [1].
I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

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

1.3.2 Registration authority – Ufficio di Registrazione (RA)

Le **Registration Authorities o Uffici di Registrazione** sono soggetti cui la CA ha conferito specifico mandato con rappresentanza con il quale affida lo svolgimento di una o più attività proprie del processo di registrazione, come ad esempio:

- l'identificazione del Titolare o del Richiedente,
- la registrazione dei dati del Titolare,
- l'inoltro dei dati del Titolare ai sistemi della CA,
- la raccolta della richiesta del certificato qualificato,
- la distribuzione e/o inizializzazione del dispositivo sicuro di firma, ove presente,
- l'attivazione della procedura di certificazione della chiave pubblica,
- la fornitura di supporto al Soggetto, al Richiedente e alla CA nelle eventuali fasi di rinnovo, revoca, sospensione dei certificati.

La Registration Authority può svolgere, in sostanza tutte le attività di interfaccia tra la Certification Authority e il Titolare o il Richiedente, in base agli accordi intercorsi. Il mandato con rappresentanza, detto "Convenzione RAO", regolamenta il tipo di attività affidate dalla CA alla RA e le modalità operative di svolgimento.

Le RA sono attivate dalla CA a seguito di un adeguato addestramento del personale impiegato; la CA verifica la rispondenza delle procedure utilizzate a quanto stabilito dal presente Manuale.

1.3.2.1 Incaricato alla Registrazione (IR)

La RA può nominare persone fisiche o giuridiche cui affidare lo svolgimento delle attività di

identificazione del Titolare, registrazione e inoltro dei dati del Titolare ai sistemi della CA. Gli **Incaricati alla Registrazione** operano sulla base delle istruzioni ricevute dalla RA, cui fanno riferimento e che ha compiti di vigilanza sulla correttezza delle procedure attuate.

1.3.3 Titolare

È la persona fisica titolare del certificato qualificato, all'interno del quale sono inseriti i dati identificativi fondamentali.

1.3.4 Utente

È il soggetto che riceve un documento informatico sottoscritto con il certificato digitale del Titolare, e che fa affidamento sulla validità del certificato medesimo (e/o sulla firma digitale ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

1.3.5 Richiedente

È la persona fisica o giuridica che richiede alla CA il rilascio di certificati digitali per un Titolare, eventualmente sostenendone i costi e assumendo la facoltà di sospendere o revocare i certificati stessi.
Nello specifico si individuano le seguenti casistiche:

- Può coincidere con il Titolare se questi è una persona fisica;
- Può essere la persona giuridica che richiede il certificato per persone fisiche a essa legate da rapporti commerciali ovvero nell'ambito di organizzazioni.

Il Richiedente può essere la persona fisica o giuridica da cui discendono i poteri di firma o il ruolo del Titolare. In questo caso, dove il Richiedente viene anche definito Terzo Interessato, nel certificato viene inserita l'indicazione dell'Organizzazione a cui il Titolare stesso è collegato, e/o del ruolo.
Se non specificato altrimenti nella documentazione contrattuale, il Richiedente coincide con il Titolare.

1.3.6 Autorità

1.3.6.1 Agenzia per l'Italia Digitale - AgID

L'Agenzia per l'Italia Digitale (**AgID**), è l'organismo di vigilanza sui prestatori di servizi fiduciari, ai sensi dell'articolo 17 del Regolamento eIDAS. In tale veste, AgID effettua la vigilanza sui prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano al fine di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

1.3.6.2 Organismo di valutazione della conformità - Conformity Assessment Body

L'organismo di valutazione della conformità (**CAB**, acronimo di Conformity Assessment Body) è un organismo accreditato secondo quanto previsto dal Regolamento eIDAS, che è competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

1.4 Uso del certificato

1.4.1 Usi consentiti

I certificati emessi dalla CA Zucchetti, secondo le modalità indicate dal presente manuale operativo, sono Certificati Qualificati ai sensi del CAD [1] e del Regolamento Eidas [1].

Il certificato emesso dalla CA sarà usato per verificare la firma qualificata del Titolare cui il certificato

appartiene.

La CA Zucchetti mette a disposizione per la verifica delle firme il prodotto descritto all'Appendice C. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

1.4.2 Usi non consentiti

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel Manuale Operativo e dai contratti, e comunque in violazione dei limiti d'uso e di valore (*key usage*, *extended key usage usernotice*) previsti.

1.5 Amministrazione del Manuale Operativo

1.5.1 Contatti

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.

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dall'Ufficio Legale e approvato dal management aziendale.

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001.
Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

1.6 Definizioni e acronimi

1.6.1 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal Regolamento eIDAS [1] e dal CAD [1] 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.

Termine	Definizione
Autocertificazione	È la dichiarazione, rivolta alla CA, effettuata personalmente dal soggetto che risulterà Titolare del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità con assunzione delle responsabilità stabilite per legge.
CAB – Conformity Assessment Body (Organismo di valutazione della conformità)	organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
CAR – Conformity Assessment Report (Relazione di valutazione della conformità)	relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr eIDAS [1]).
certificato di firma elettronica	un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona (cfr eIDAS [1])
certificato qualificato di firma elettronica	un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (cfr eIDAS [1])
chiave di certificazione o chiave di root	coppia di chiavi crittografiche utilizzate dalla CA per firmare i certificati e le liste dei certificati revocati o sospesi
chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante la quale si appone la firma digitale sul documento informatico (cfr CAD [1].)
chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare (cfr CAD [1])
codice di emergenza (ERC)	Codice di sicurezza consegnato al Titolare per inoltrare la richiesta di sospensione di un certificato sui portali del TSP
Convalida	il processo di verifica e conferma della validità di una firma (cfr eIDAS [1])
dati di convalida	dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1])
dati di identificazione personale	un insieme di dati che consente di stabilire l'identità di una persona fisica o di una persona fisica che rappresenta una persona giuridica (cfr eIDAS [1])
dati per la creazione di una firma elettronica	i dati unici utilizzati dal firmatario per creare una firma elettronica (cfr eIDAS [1])
dispositivo per la creazione di una firma elettronica	un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1])
dispositivo per la creazione di una firma elettronica qualificata (SSCD – secure system creation device o QSCD)	un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS (cfr eIDAS [1]). L'iniziale Q sta a intendere che il dispositivo è qualificato
documento elettronico	qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1])

Termine	Definizione
firma automatica	particolare procedura informatica di firma elettronica eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
firma digitale (digital signature)	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (cfr CAD [1])
firma elettronica	dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (cfr eIDAS [1])
firma elettronica avanzata	una firma elettronica che soddisfi i requisiti di cui all'articolo 26 del Regolamento eIDAS (cfr eIDAS [1])
firma elettronica qualificata	una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr eIDAS [1])
firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse (cfr DPCM [1])
firmatario	una persona fisica che crea una firma elettronica (cfr eIDAS [1])
giornale di controllo	Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [1].
identificazione elettronica	il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica (cfr eIDAS [1]).
lista dei certificati revocati o sospesi [Certificate Revocation List - CRL]	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.
manuale operativo [certificate practice statement]	Il Manuale Operativo definisce le procedure che la CA applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.
mezzi di identificazione elettronica	un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr eIDAS [1])
Online Certificate Status Protocol (OCSP)	Protocollo definito dallo IETF nella RFC 6960, consente alle applicazioni di verificare la validità del certificato in maniera più veloce e puntuale rispetto alla CRL, di cui condivide i dati
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.
parte facente affidamento sulla certificazione	una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario (cfr eIDAS [1]).
prestatore di servizi fiduciari	una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato (cfr eIDAS [1])

Termine	Definizione
prestatore di servizi fiduciari qualificato	un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr eIDAS [1])
Prodotto	un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari (cfr eIDAS [1])
pubblico ufficiale	Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche
registro pubblico [Directory]	Il Registro pubblico è un archivio che contiene: ▪ tutti i certificati emessi dalla CA per i quali sia stata richiesta dal Soggetto la pubblicazione; ▪ la lista dei certificati revocati e sospesi (CRL).
revoca o sospensione di un certificato:	È l'operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
Ruolo	Il termine Ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del Titolare, 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	un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1])
servizio fiduciario qualificato	un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1])
Tempo Universale Coordinato [Coordinated Universal Time]:	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
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 (cfr eIDAS [1])
validazione temporale elettronica qualificata	una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS (cfr eIDAS [1])

1.6.2 Acronimi e abbreviazioni

Acronimo	
AgID	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari;
CA	Certification Authority
CAB	Conformity Assessment Body – Organismo di valutazione della conformità
CAD	Codice dell'Amministrazione Digitale
CAR	Conformity Assessment Report – Relazione di valutazione della conformità
CC	Common Criteria

Acronimo	
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguish Name
EAL	Evaluation Assurance Level
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute;
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smartcard, ma con superiori caratteristiche di memoria e di performance;
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Incaricato alla Registrazione
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: fondata nel 1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
IUT	Identificativo Univoco del Titolare: è un codice associato al Soggetto che lo identifica univocamente presso la CA; il Soggetto ha codici diversi per ogni certificato in suo possesso;
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati;
LoA	Level of Assurance
NTR Code	National Trade Register Code
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;
OTP	OneTime Password
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso;
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse, processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto

Acronimo	
RA	Registration Authority – Autorità di Registrazione
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
RSA	Deriva dalle iniziali degli inventori dell'algoritmo: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SSCD – QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una firma elettronica Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X500	Standard ITU-T per i servizi LDAP e directory
X509	Standard ITU-T per le PKI

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Archiviazione

I certificati pubblicati, le CRLs e i manuali operativi sono pubblicati e disponibili 24 ore al giorno per 7 giorni alla settimana.

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del manuale operativo

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web del Certificatore (cfr. § 1.25.1)
- 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 dalla legge sono pubblicate presso l'elenco dei certificatori.

2.2.2 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.

2.2.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: ldap://ldap.ca.zucchetti.it o con protocollo http all'indirizzo http://crl.ca.zucchetti.it.
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 dalla CA 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.

2.3 Periodo o frequenza di pubblicazione

2.3.1 Frequenza di pubblicazione del manuale operativo

Il manuale operativo viene pubblicato con frequenza variabile se sono subentrati dei cambiamenti. Se i cambiamenti sono importanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

Le CRLs vengono pubblicate ogni ora.

2.4 Controllo degli accessi agli archivi pubblici

Le informazioni relative ai certificati pubblicati, alle CRLs e i manuali operativi sono pubbliche, la CA non ha messo restrizione all'accesso in lettura e ha attuato tutte le contromisure per scongiurare modifiche/cancellazioni non autorizzate.

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

Il soggetto nel certificato è identificato con l'attributo Subject Distinguished Name che, quindi, deve essere valorizzato e conforme allo standard X500. I certificati vengono emessi secondo gli standard ETSI per l'emissione dei certificati qualificati e secondo le indicazioni presenti nel DPCM.

3.1.2 Necessità che il nome abbia un significato

L'attributo del certificato Subject Distinguished Name identifica in maniera univoca il soggetto a cui è rilasciato il certificato.

3.1.3 Anonimato e pseudonimia dei richiedenti

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

3.1.4 Regole di interpretazione dei tipi di nomi

Zucchetti si attiene allo standard X500.

3.1.5 Univocità dei nomi

Nel caso di persona fisica, per garantire l'univocità del Soggetto, nel certificato deve essere indicato il nome e cognome e un codice identificativo univoco, ossia il TIN – Tax Identification Number. Il TIN viene assegnato dalle autorità del Paese di cui il Titolare è cittadino ovvero dal Paese in cui ha sede l'organizzazione in cui esso lavora.
Per i cittadini italiani il codice identificativo univoco è il codice fiscale.
In assenza di Codice Fiscale o TIN, nel certificato potrà essere inserito un codice identificativo tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento.

3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

Il Titolare e il Richiedente, quando richiedono un certificato alla CA garantiscono di operare nel pieno rispetto delle normative nazionali e internazionali sulla proprietà intellettuale.

La CA non fa verifiche sull'utilizzo di marchi, e può rifiutarsi di revocare un certificato coinvolto in una disputa.

3.2 Convalida iniziale dell'identità

Questo capitolo descrive le procedure usate per l'identificazione del Titolare o del Richiedente al momento della richiesta di rilascio del certificato qualificato.

La procedura di identificazione comporta che il Titolare sia riconosciuto dalla CA, anche attraverso la RA o un suo Incaricato, che ne verificherà l'identità attraverso una delle modalità definite nel Manuale Operativo.

3.2.1 Metodo per dimostrare il possesso della chiave privata

Zucchetti stabilisce che il richiedente possiede o controlla la chiave privata corrispondente alla chiave pubblica da certificare, verificando la firma della richiesta di certificato tramite la chiave privata corrispondente alla chiave pubblica da certificare

3.2.2 Autenticazione dell'identità delle organizzazioni

n/a

3.2.3 Identificazione della persona fisica

Ferma restando la responsabilità della CA, l'identità del Titolare può essere accertata dai soggetti abilitati ad eseguire il riconoscimento, attraverso le seguenti modalità:

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
1 De Visu	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione • Pubblico Ufficiale • Datore di Lavoro per la identificazione dei propri dipendenti, collaboratori, agenti	n/a
2 Firma Digitale	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	Utilizzo di una firma elettronica qualificata emessa da un Prestatore di Servizi Fiduciari Qualificato

3.2.3.1 Riconoscimento effettuato secondo la modalità 1 – De Visu

La modalità di identificazione **De Visu** prevede un incontro di persona tra il Titolare, che deve aver compiuto 18 anni di età, e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti d'identificazione in corso di validità[1]. Per garantire l'univocità del Titolare e del relativo nome, questi deve essere in possesso anche del codice identificativo univoco di cui al paragrafo 3.1.5. Il soggetto abilitato ad eseguire il riconoscimento può richiedere l'esibizione di documentazione che comprovi il possesso di tale identificativo univoco. Le Registration Authority operanti all'estero, o che comunque identificano Soggetti residenti all'estero, possono essere autorizzate da Zucchetti ad accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte della Autorità Emittenti, nonché specifica formazione[2].
L'identificazione può essere eseguita anche da parte di un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività. Il Titolare compila la richiesta di Certificazione e la sottoscrive di fronte ad un Pubblico Ufficiale, facendo autenticare la propria firma ai sensi delle normative vigenti. La richiesta è poi presentata alla CA ad uno degli Uffici di Registrazione convenzionati.
L'identificazione già eseguita dal datore di lavoro, ai fini della stipula del contratto di lavoro, è considerata valida dalla CA in conformità con la seguente modalità di riconoscimento, previa verifica delle procedure operative di identificazione e di autenticazione. Analogamente, è considerata valida in conformità alla seguente modalità di riconoscimento, l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia, previa verifica delle procedure operative di

[1] Per l'Italia sono i documenti previsti dal DPR 445/2000 e s.m.i. (Testo Unico Documentazione Amministrativa). I titolari con cittadinanza diversa da quella italiana, ai fini dell'identificazione esibiscono in originale uno dei seguenti documenti d'identificazione:
- passaporto,
- carta di identità italiana (se cittadini europei).

[2] Tali casi saranno comunicati all'Autorità di Vigilanza (AgID)

identificazione e di autenticazione.
Questa modalità di identificazione prevede il conferimento da parte della CA di un mandato con rappresentanza al datore di lavoro, che agisce quindi da RA[3]. I Certificati emessi secondo questa modalità di identificazione possono essere utilizzati solamente per le finalità di lavoro per le quali sono rilasciati, e contengono uno specifico limite d'uso.
I dati di registrazione per la modalità di identificazione De Visu sono conservati dalla CA in formato analogico o in formato elettronico per 20 anni dalla scadenza del certificato.

3.2.3.2 Riconoscimento effettuato secondo la modalità 2 – Firma Digitale

Nella **modalità 2 Firma Digitale** la CA Zucchetti si basa sul riconoscimento già effettuato da un'altra CA che emette certificati qualificati. Il Soggetto è già in possesso di un certificato qualificato ancora in corso di validità, che utilizza nei confronti di Zucchetti. I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

3.2.4 Identificazione della persona giuridica

n/a

3.2.5 Informazioni del Titolare o del Richiedente non verificate

Il Titolare può ottenere, direttamente o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di informazioni relative a:

- 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 con il Ruolo è conforme a quanto indicato nella Deliberazione 45 [1]. Il Titolare deve produrre la dichiarazione idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo mediante Autocertificazione[4]. La CA non assume alcuna responsabilità, salvo i casi di dolo o colpa , in merito all'inserimento nel certificato delle informazioni autocertificate dal Soggetto.

La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se essa ha autorizzato il rilascio del certificato al Soggetto, anche senza l'esplicita indicazione di un ruolo. In tale ipotesi la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Soggetto. La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni in possesso di Codice Fiscale o Partita IVA, ovvero VAT Code.

3.2.5.1 Titoli e/o Abilitazioni Professionali

Nel caso in cui sia richiesta l'indicazione nel certificato di Abilitazioni Professionali per l'esercizio delle quali sia necessario ottenere preventivamente l'iscrizione all'Albo su verifica dell'Ordine professionale competente alla tenuta e vigilanza dello stesso, il Titolare, salvo diversa pattuizione tra il

[3] Prima del conferimento del mandato, la CA esegue una attenta valutazione della sicurezza delle procedure di identificazione del dipendente e della modalità di assegnazione e gestione degli strumenti di identificazione personale ai sistemi informatici cui il dipendente (o agente, o dipendente in stato di pensione) accede per richiedere alla CA il certificato di firma digitale. Tali casi saranno comunicati all'Autorità di Vigilanza (AgID).

[4] Nel caso in cui la richiesta di inserimento del ruolo nel certificato sia stata effettuata mediante la sola autocertificazione da parte del Soggetto, il certificato non riporterà informazioni inerenti l'organizzazione a cui potrebbe eventualmente essere legato il ruolo stesso.

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.

3.2.5.2 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.

3.2.5.3 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.

3.2.6 Validazione dell'autorità

La CA ovvero la RA verificano le informazioni richieste, definite nei paragrafi 3.2.3 e 3.2.4, per l'identificazione e validano la richiesta.

3.3 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati

3.3.1 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati

Questo paragrafo descrive le procedure usate per l'autenticazione e identificazione del Titolare nel caso di rinnovo del certificato qualificato di firma.

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

Il Titolare può, tuttavia, rinnovarlo, prima della sua scadenza, utilizzando gli strumenti messi a disposizione dalla CA, che presentano una richiesta di rinnovo che viene sottoscritta con la chiave privata corrispondente alla chiave pubblica contenuta nel certificato da rinnovare. Dopo la revoca o la scadenza del certificato non è possibile eseguire il rinnovo del certificato, diventando quindi necessaria una nuova emissione.

3.4 Identificazione e autenticazione per le richieste di revoca o sospensione

La revoca o sospensione del certificato può avvenire su richiesta del Titolare o del Richiedente (Terzo Interessato nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo) ovvero su iniziativa della CA.

3.4.1 Richiesta da parte del Titolare

Il Titolare può richiedere la revoca o sospensione compilando e sottoscrivendo anche digitalmente il modulo presente sul sito della CA.

La richiesta di sospensione può essere fatta attraverso un form Internet, in tal caso il Titolare si autentica fornendo il codice di emergenza consegnato al momento dell'emissione del certificato, oppure con un altro sistema di autenticazione descritto nella documentazione contrattuale consegnata all'atto della registrazione.

Se la richiesta viene fatta presso la Registration Authority, l'autenticazione del Titolare avviene con le modalità previste per l'identificazione.

3.4.2 Richiesta da parte del Richiedente

Il Richiedente che richiede la revoca o sospensione del certificato del Soggetto si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dalla CA.

La richiesta dovrà essere inoltrata con le modalità indicate ai paragrafi 4.9.3.2 o 4.9.15.2. La CA si riserva di individuare ulteriori modalità di inoltro della richiesta, di revoca o sospensione del Richiedente o del Terzo Interessato in apposite convenzioni da stipulare con lo stesso.

4 OPERATIVITÀ

4.1 Richiesta del certificato

4.1.1 Chi può richiedere un certificato

Il certificato qualificato per una persona fisica può essere richiesto da:

- Il Titolare,
  - rivolgendosi direttamente alla CA al sito www.firmadigitale.zucchetti.it, ovvero
  - rivolgendosi a una Registration Authority
- Il Richiedente per conto del Titolare
  - rivolgendosi direttamente alla CA mediante il sito www.firmadigitale.zucchetti.it o stipulando un accordo commerciale con la CA
  - rivolgendosi a una Registration Authority

4.1.2 Processo di registrazione e responsabilità

Il processo di registrazione comprende: la richiesta da parte del Titolare, la generazione della coppia di chiavi, la richiesta di certificazione della chiave pubblica e la firma dei contratti, non necessariamente in quest'ordine. Nel processo, i diversi attori hanno responsabilità differenziate e concorrono congiuntamente al buon esito dell'emissione:

- Il Titolare ha la responsabilità di fornire informazioni corrette e veritiere sulla propria identità, di leggere attentamente il materiale messo a disposizione dalla CA, anche attraverso la RA, di seguire le istruzioni della CA e/o della RA nell'avanzare la richiesta del certificato qualificato;
- Il Richiedente, ove presente, ha la responsabilità di informare il Titolare, per conto del quale sta richiedendo il certificato, sugli obblighi derivanti dal certificato, di fornire le informazioni corrette e veritiere sull'identità del Titolare, di seguire i processi e le indicazioni della CA e/o della RA;
- La Registration Authority, dove presente e anche attraverso l'Incaricato alla Registrazione, ha la responsabilità di identificare con certezza il Titolare e il Richiedente, informare i vari soggetti sugli obblighi derivanti dal certificato e seguire dettagliatamente i processi definiti dalla CA;
- La Certification Authority è il responsabile ultimo della identificazione del Titolare e del buon esito del processo di iscrizione del certificato qualificato.

4.2 Elaborazione della richiesta

Per ottenere un certificato di sottoscrizione il Titolare e/o il Richiedente deve:

- prendere visione del presente Manuale Operativo, della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel paragrafo;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

4.2.1 Informazioni che il Titolare deve fornire

4.2.1.1 Persona fisica

Per la richiesta di un certificato qualificato di sottoscrizione il Titolare o il Richiedente che richiede il certificato della persona fisica deve fornire obbligatoriamente le seguenti informazioni:

- Cognome e Nome;
- Data e luogo di nascita;
- Codice TIN (codice fiscale nel contesto italiano) o, in sua assenza analogo codice identificativo quale il numero del documento d'identità;
- Indirizzo di residenza;
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- e-mail per l'invio delle comunicazioni dalla CA al Titolare;
- numero di telefonia mobile per la trasmissione della OTP ove fosse questa la tecnologia OTP adottata.

Opzionalmente il Titolare (o il Richiedente) 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 Soggetto o dal Richiedente, sarà valorizzato con nome e cognome del Soggetto stesso.

4.2.1.1 Persona giuridica

n/a

4.2.2 Esecuzione delle funzioni di identificazione e autenticazione

Durante la fase di registrazione iniziale e raccolta della richiesta di registrazione e certificazione vengono consegnati al Titolare i codici di sicurezza che gli consentono sia di procedere alla attivazione del dispositivo di firma o della procedura di firma, se remota, e alla eventuale richiesta di sospensione del certificato (codice ERC o codice analogo, se previsto dal contratto). I codici di sicurezza sono consegnati in busta cieca ovvero, se elettronici, trasmessi all'interno di file cifrati.
La CA può prevedere che il PIN di firma sia scelto in autonomia dal Titolare; in tali casi è onere del Titolare ricordare il PIN.

4.2.3 Approvazione o rifiuto della richiesta del certificato

Dopo la registrazione iniziale la CA o la RA possono rifiutarsi di portare a termine l'emissione del certificato di sottoscrizione in caso di assenza o incompletezza di informazioni, verifiche di coerenza e consistenza delle informazioni fornite, verifiche anti-frode, dubbi sull'identità del Titolare o del Richiedente, ecc.

4.2.4 Tempo massimo per l'elaborazione della richiesta del certificato

Il tempo che intercorre dal momento della richiesta di registrazione al momento di emissione del certificato dipende dalla modalità di richiesta prescelta dal Titolare e dalla eventuale necessità di raccogliere ulteriori informazioni ovvero di consegnare fisicamente il dispositivo.

4.3 Emissione del certificato

4.3.1 Azioni della CA durante l'emissione del certificato

4.3.1.1 Emissione del certificato su dispositivo di firma (smartcard o token)

La coppia di chiavi crittografiche viene generata dalla RA direttamente sui dispositivi sicuri di firma, utilizzando le applicazioni messe a disposizione dalla CA, previa autenticazione sicura.

La RA invia alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10 firmata digitalmente con il certificato qualificato di sottoscrizione specificatamente autorizzato a tal fine.

La Certification Authority, verificata la validità della firma sul PKCS#10 e la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che è inviato su canale sicuro all'interno del dispositivo.

4.3.1.2 Emissione del certificato su dispositivo di firma remota (HSM)

Il Titolare si autentica ai servizi o alle applicazioni messe a disposizione dalla RA.

La coppia di chiavi crittografiche viene generata dalla RA direttamente sull'HSM; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10, che è firmata digitalmente con il certificato qualificato di sottoscrizione per procedura automatica specificatamente autorizzato a tal fine.

La Certification Authority, verificata la validità della firma sul PKCS#10 e la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che viene memorizzato sull'HSM stesso.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

In caso di emissione su dispositivo crittografico il Titolare non ha bisogno di notifica poiché il certificato è presente nel dispositivo che ha ricevuto. Negli altri casi riceverà la notifica attraverso l'indirizzo email che ha indicato al momento dell'iscrizione.

4.3.3 Attivazione

4.3.3.1 Attivazione del dispositivo di firma (smartcard o token)

Dopo la ricezione del dispositivo il Titolare, utilizzando i codici di attivazione ricevuti in maniera riservata e l'apposito software messo a disposizione dalla CA, procede ad attivare il dispositivo scegliendo contestualmente il PIN di firma, quantità di sicurezza riservata la cui custodia e tutela è posta esclusivamente in capo al Titolare stesso.

4.3.3.2 Attivazione del dispositivo di firma remota (HSM)

Il Titolare autenticato ai portali della CA attraverso i codici di attivazione ricevuti in maniera riservata, digita il PIN di firma, quantità di sicurezza riservata la cui custodia e tutela è posta esclusivamente in capo al Soggetto stesso, che viene confermato con l'inserimento della OneTime Password ricevuta via SMS, ovvero generata sul token o la token-app associata al certificato.

4.4 Accettazione del certificato

4.4.1 Comportamenti concludenti di accettazione del certificato

n/a

4.4.2 Pubblicazione del certificato da parte della Certification Authority

Al buon esito della procedura di certificazione, il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico. Il Titolare che volesse rendere pubblico il proprio certificato potrà richiederlo tramite la procedura descritta al §2.2.2. La richiesta verrà evasa entro tre giorni lavorativi

4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato

n/a

4.5 Uso della coppia di chiavi e del certificato

4.5.1 Uso della chiave privata e del certificato da parte del Titolare

Il Titolare deve custodire in maniera sicura il dispositivo di firma, se presente, ovvero gli strumenti di autenticazione per la firma remota; deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo. Deve garantire la protezione della segretezza e la conservazione del codice di emergenza necessario alla sospensione del certificato, deve utilizzare il certificato per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.
Non deve apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato e non deve apporre firme elettroniche avvalendosi di certificato emesso da CA revocata.

4.5.2 Uso della chiave pubblica e del certificato da parte degli Utenti Finali

L'Utente Finale deve conoscere l'ambito di utilizzo del certificato riportati nel Manuale Operativo e nel certificato stesso. Deve verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta e che il certificato non risulti sospeso o revocato controllando le relative liste nel registro dei certificati, deve inoltre verificare l'esistenza ed il contenuto di eventuali limitazioni d'uso della coppia di chiavi, poteri di rappresentanza ed abilitazioni professionali.

4.5.3 Limiti d'uso e di valore

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:
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.
- I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato.
  The certificate holder must use the certificate only for the purposes for which it is issued.

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

È inoltre facoltà del Soggetto o del Richiedente richiedere alla Certification Authority l'inserimento nel certificato di limiti d'uso personalizzati. La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dalla CA per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.

È inoltre facoltà del Soggetto richiedere alla CA 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.

La CA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Ferma restando la responsabilità della CA di cui al CAD (art.30), è responsabilità dell'Utente verificare il rispetto dei limiti d'uso e di valore inseriti nel certificato.

4.6 Rinnovo del certificato

4.6.1 Motivi per il rinnovo

Il rinnovo consente di ottenere un nuovo certificato di sottoscrizione da utilizzare per firmare documenti e transazioni.

4.6.2 Chi può richiedere il rinnovo

Il Titolare può richiedere il rinnovo del certificato prima della sua scadenza solo se non è stato revocato e se tutte le informazioni fornite all'atto della emissione precedente sono ancora valide; oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla richiesta di un nuovo certificato.
La procedura di rinnovo si applica esclusivamente a certificati emessi da Zucchetti.
Il rinnovo di certificato per firma automatica non è previsto e si dovrà procedere ad una nuova emissione.

4.6.3 Elaborazione della richiesta di rinnovo del certificato

Il rinnovo viene eseguito attraverso un servizio messo disposizione dalla CA, nell'ambito dei rapporti commerciali e contrattuali definiti con il Titolare e con la RA, dove presente.

4.7 Riemissione del certificato

n/a

4.8 Modifica del certificato

n/a

4.9 Revoca e sospensione del certificato

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e rendono non valide le firme apposte successivamente al momento della pubblicazione della revoca. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dalla CA che li ha emessi, pubblicata nel registro dei certificati con periodicità prestabilita. La CA 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 della Certification Authority.

4.9.1 Motivi per la revoca

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) oppure, per i certificati di firma remota, sia stato compromesso o smarrito il dispositivo OTP;
   - 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, ad esempio per un guasto;
3. si verifica un cambiamento dei dati del Titolare presenti nel certificato, ivi compresi quelli relativi al Ruolo, tale da rendere detti dati non più corretti e/o veritieri;
4. termina il rapporto tra il Titolare e la CA, ovvero tra il Richiedente e la CA;
5. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

4.9.2 Chi può richiedere la revoca

La revoca può essere richiesta dal Titolare in qualsiasi momento e per un qualunque motivo. Inoltre, la revoca del certificato può essere richiesta anche dal Richiedente o Terzo Interessato, per i motivi e nelle modalità previsti dal presente Manuale Operativo. Infine, il certificato può essere revocato d'ufficio dalla CA.

4.9.3 Procedure per richiedere la revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del soggetto che la pone in essere.

4.9.3.1 Revoca richiesta dal Titolare

Il Titolare è tenuto a sottoscrivere la richiesta di revoca, utilizzando il modulo presente nel sito Zucchetti consegnarla alla RA o inviarla direttamente alla CA per posta raccomandata, PEC o fax, corredata di una fotocopia di un documento di identità in corso di validità.

La CA verifica l'autenticità della richiesta, procede alla revoca del certificato, dandone immediata notizia al Titolare.

La CA, qualora nel certificato oggetto della richiesta di revoca siano presenti informazioni relative al Ruolo del Titolare, provvederà a comunicare l'avvenuta revoca all'eventuale Terzo Interessato con cui siano operative le specifiche convenzioni. La CA qualora nel certificato oggetto della richiesta di

revoca sia presente l'indicazione dell'Organizzazione, provvederà a comunicare l'avvenuta revoca a tale soggetto.

4.9.3.2 Revoca richiesta dal Richiedente o dal Terzo Interessato

Il Richiedente può richiedere la revoca del certificato del Soggetto compilando l'apposito modulo messo a disposizione sul sito della CA e presso le RA, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del Titolare del certificato comunicati alla CA al momento dell'emissione del certificato. La richiesta deve essere resa per iscritto.

La CA verifica l'autenticità della richiesta, ne dà notizia al Titolare utilizzando il mezzo di comunicazione stabilito all'atto della richiesta del certificato e procede alla revoca del certificato.

Modalità aggiuntive per la richiesta di revoca da parte del Richiedente o dal Terzo Interessato potranno essere specificate negli eventuali accordi stipulati con la CA.

4.9.3.3 Revoca su iniziativa della Certification Authority

Qualora se ne verifichi la necessità, la CA ha facoltà di revocare il certificato, comunicandolo preventivamente al Titolare, fornendo il motivo della revoca, nonché la data e l'ora di decorrenza.

La CA, qualora nel certificato oggetto della revoca siano presenti informazioni relative al Ruolo del Titolare, provvederà a comunicare l'avvenuta revoca all'eventuale Terzo Interessato con cui siano operative le specifiche convenzioni. Qualora nel certificato oggetto della richiesta di revoca sia presente l'indicazione dell'Organizzazione, la CA provvederà a comunicare l'avvenuta revoca a tale soggetto.

4.9.4 Periodo di grazia della richiesta di revoca

Il periodo di grazia della CRL è il periodo di tempo che intercorre tra il momento della pubblicazione da parte della CA della successiva CRL e il momento in cui scade la CRL corrente. Per non causare disservizi ad ogni parte coinvolta, questo periodo è più lungo del periodo di tempo di cui la CA ha bisogno per generare e pubblicare una nuova CRL. In questo modo la CRL corrente rimane valida almeno fino a quando non viene sostituita dalla nuova CRL.

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

La richiesta viene evasa entro 24 ore, a meno che non siano necessari ulteriori controlli sull'autenticità della stessa. Se la richiesta viene autenticata correttamente viene elaborata immediatamente altrimenti si provvede alla sospensione del certificato in attesa di eseguire ulteriori accertamenti sull'autenticità della richiesta ricevuta.

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dalla CA, e pubblicata nel Registro pubblico. La CRL viene pubblicata in modo programmato ogni ora (emissione ordinaria).
La CA 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 di Time Stamping Authority Zucchetti 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.
La CA 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.

4.9.8 Latenza massima della CRL

Il tempo di attesa tra l'accettazione da parte della CA della richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di un'ora.

4.9.9 Servizi online di verifica dello stato di revoca del certificato

Oltre alla pubblicazione della CRL nei registri LDAP e HTTP, Zucchetti mette a disposizione anche un servizio OCSP per la verifica dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 X 7.

4.9.10 Requisiti servizi on line di verifica

Si veda l'Appendice B.

4.9.11 Altre forme di revoca

n/a

4.9.12 Requisiti specifici rekey in caso di compromissione

n/a

4.9.13 Motivi per la sospensione

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 Richiedente o Terzo Interessato, la RA o la CA hanno acquisito elementi di dubbio sulla validità del certificato;
3. siano insorti dubbi sulla sicurezza del dispositivo OTP, ove presente
4. è necessaria un'interruzione temporanea della validità del certificato.

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

4.9.14 Chi può richiedere la sospensione

La sospensione può essere richiesta dal Titolare in qualsiasi momento e per un qualunque motivo. Inoltre, la sospensione del certificato può essere richiesta anche dal Richiedente o dal Terzo Interessato, per i motivi e nelle modalità previsti dal presente Manuale Operativo. Infine, il certificato può essere sospeso d'ufficio dalla CA.

4.9.15 Procedure per richiedere la 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.

4.9.15.1 Sospensione richiesta dal Titolare

Il Titolare deve richiedere la sospensione con una delle seguenti modalità:

1. utilizzando la funzione di sospensione disponibile nel sito web della CA, comunicando i dati richiesti e utilizzando il codice di emergenza fornito in sede di emissione del certificato,
2. telefonando al Call Center della CA e fornendo le informazioni richieste. 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 Soggetto; qualora la CA non riceva la richiesta sottoscritta entro il termine indicato, procede a riattivare il certificato.
3. tramite la Registration Authority, la quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione alla CA. Il Soggetto è tenuto a sottoscrivere la richiesta di sospensione e consegnarla alla RA o inviarla direttamente alla CA per posta ordinaria, PEC o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

La CA, qualora nel certificato oggetto della richiesta di sospensione siano presenti informazioni relative al Ruolo del Titolare, provvederà a comunicare l'avvenuta sospensione all'eventuale Terzo Interessato con cui siano operative le specifiche convenzioni. La CA, qualora nel certificato oggetto della richiesta di sospensione sia presente l'indicazione dell'Organizzazione, provvederà a comunicare l'avvenuta sospensione a tale soggetto.

4.9.15.2 Sospensione richiesta dal Richiedente o dal Terzo Interessato

Il Richiedente o il Terzo Interessato possono richiedere la sospensione del certificato del Titolare compilando l'apposito modulo messo a disposizione sul sito della CA e presso le RA, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del Titolare comunicati alla CA al momento dell'emissione del certificato.

La CA verifica l'autenticità della richiesta, ne dà notizia al Titolare secondo le modalità di comunicazione stabilite all'atto della richiesta del certificato e procede alla sospensione. Modalità aggiuntive per la richiesta di sospensione da parte del Richiedente o del Terzo Interessato potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo e la CA.

4.9.15.3 Sospensione su iniziativa della CA

La CA, salvo casi d'urgenza, comunica preventivamente al Titolare l'intenzione di sospendere il certificato, fornendo il motivo della sospensione, la data di decorrenza e la data di termine. Queste ultime informazioni saranno in ogni caso comunicate al più presto al Titolare.
La CA, qualora nel certificato oggetto della sospensione siano presenti informazioni relative al Ruolo del Titolare, provvederà a comunicare l'avvenuta sospensione all'eventuale Terzo Interessato con cui siano operative le specifiche convenzioni. La CA, qualora nel certificato oggetto della sospensione sia presente l'indicazione dell'Organizzazione, provvederà a comunicare l'avvenuta sospensione a tale soggetto.

4.9.16 Limiti al periodo di sospensione

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 il giorno di scadenza della sospensione coincida con il giorno di scadenza del certificato o sia a questa successivo, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

4.10 Servizi riguardanti lo stato del certificato

4.10.1 Caratteristiche operative

Le informazioni sullo stato dei certificati sono disponibili tramite CRL e servizio OCSP.
Il numero di serie di un certificato revocato rimane in CRL anche dopo la fine della validità del certificato ed almeno sino alla scadenza del certificato di CA.

Le informazioni fornite dal servizio OCSP per i certificati sono aggiornate all'ultima CRL pubblicata.

4.10.2 Disponibilità del servizio

Il servizio OCSP e le CRL sono disponibili 24 ore per 7 giorni la settimana

4.10.3 Caratteristiche opzionali

n/a

4.11 Disdetta dai servizi della CA

Il rapporto del Titolare e/o del Richiedente con la Certification Authority finisce quando il certificato scade o viene revocato, salvo casi particolari definiti a livello contrattuale.

4.12 Deposito presso terzi e recovery della chiave

n/a

5 MISURE DI SICUREZZA E CONTROLLI

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

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui la CA 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.

Un estratto della politica di sicurezza Zucchetti è disponibile sul sito www.zucchetti.it.

5.1 Sicurezza fisica

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

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

5.1.1 Posizione e costruzione della struttura

Il Data Center utilizzato da Zucchetti si trova a Padova. Il sito di Disaster Recovery è ubicato a Modena ed è connesso al Data Center sopra citato tramite un collegamento dedicato e ridondato su due circuiti diversi MPLS a 10 Gbit/s upgradabile fino a 100 Gbit/s.

All'interno di entrambi i siti sono stati ricavati dei locali protetti con dei più elevati livelli di sicurezza, sia fisici che logici, all'interno dei quali sono attestati gli apparati informatici che costituiscono il cuore dei servizi di certificazione digitale, marcatura temporale, firma remota e automatica.

5.1.2 Accesso fisico

L'accesso al Data Center è regolato da procedure di sicurezza. All'interno del Data Center c'è l'area bunker in cui sono i sistemi della CA, per il quale è richiesto un ulteriore fattore di sicurezza

5.1.3 Impianto elettrico e di climatizzazione

I locali tecnici sono provvisti di un sistema di alimentazione elettrica progettato al fine di prevenire guasti e soprattutto disservizi. L'alimentazione dei sistemi include le più moderne tecnologie al fine di incrementare l'affidabilità e assicurare la ridondanza delle funzionalità più critiche ai fini dei servizi erogati.

L'infrastruttura preposta all'alimentazione include:

- Gruppi di continuità, dotati di accumulatori, in corrente alternata (UPS);
- Disponibilità di tensione alternata (220-380V AC);

- Armadi alimentati in ridondanza con linee protette e dimensionate per l'assorbimento concordato;
- Servizio di generatori di emergenza;
- Sistema di commutazione automatico e sincronizzazione fra generatori, rete e batterie (STS).

Ogni armadio tecnologico installato presso il Data Center fruisce di due linee elettriche che assicurano l'HA in caso di interruzione di una delle due linee disponibili.

L'armadio tecnologico è monitorato remotamente; vengono effettuati controlli costanti sullo stato della linea elettrica (on/off) e le potenze elettriche assorbite (ogni linea non deve superare il 50% del carico).

L'area tecnica è normalmente mantenuta fra 20° e 27° con un tasso di umidità relativo compreso fra il 30% ed il 60%. Gli impianti sono dotati di batterie condensanti con sistema di raccolta e scarico condensa sigillato e controllato da sonde anti-allagamento. L'intero sistema di condizionamento è asservito ai generatori di emergenza in caso di assenza di energia elettrica. Si garantisce la capacità frigorifera per armadio con un carico massimo previsto di 10KW e massimo di 15 KW su due armadi affiancati.

5.1.4 Prevenzione e protezione contro gli allagamenti

La zona d'ubicazione dell'immobile non presenta rischi ambientali dovuti alla vicinanza ad installazioni "pericolose". Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica.
L'area che ospita gli apparati è al piano terreno in una posizione sopraelevata rispetto al livello della strada.

5.1.5 Prevenzione e protezione contro gli incendi

È presente nel Data Center un impianto di rilevazione fumi gestito da centrale analogica indirizzata NOTIFIER con sensori ottici posizionati in ambiente e nel controsoffitto e sensori a campionamento d'aria installati sottopavimento e nelle canalizzazioni dell'aria.
L'impianto di rilevazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici NAFS125 e PF23 e, in alcune sale, con sistemi di spegnimento ad aerosol.
Nel caso di intervento contemporaneo di due rivelatori nella stessa zona, è comandata la scarica di estinguente nella zona interessata.
Per ogni compartimento antincendio è previsto un impianto di estinzione dedicato.
Sono inoltre presenti mezzi estinguenti portatili in conformità alle leggi e normative vigenti.
Le canalizzazioni dell'aria primaria asservite alle sale apparati sono dotate, in corrispondenza degli attraversamenti dei compartimenti antincendio, di serrande tagliafuoco azionate dall'impianto automatico di rilevazione incendi.

5.1.6 Supporti di memorizzazione

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp (FAS 8060). Per la parte SAN si è invece implementata un'infrastruttura basata su tecnologie EMC2 che comprendono VNX 7600, VNX 5200, XtremIO, gestite attraverso il layer di virtualizzazione storage VPLEX. Tale infrastruttura viene gestita attraverso ViPR.

5.1.7 Smaltimento dei rifiuti

Lo smaltimento dei rifiuti avviene rispettando la normativa di riferimento. Per quel che riguarda il contenuto informativo dei rifiuti elettronici, tutti i media, prima della dismissione, vengono ripuliti secondo le procedure previste ovvero avvelandosi di società di sanitizzazione certificate.

5.1.8 Off-site backup

È realizzato nel sito di Disaster Recovery, con un dispositivo EMC Data Domain 4200, su cui, il Data Domain primario del sito di Padova, replica i dati di backup.

5.2 Controlli procedurali

5.2.1 Ruoli chiave

I ruoli chiave sono coperti da figure dotate dei necessari requisiti di esperienza, professionalità e competenza tecnica e giuridica, che vengono continuamente verificati mediante le valutazioni annuali.
La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

5.3 Controllo del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

Il Responsabile Funzione/Struttura Organizzativa identifica le caratteristiche e gli skill della risorsa da inserire. Successivamente, di concerto con l'Ufficio Risorse Umane, viene attivato il processo di ricerca e selezione.
Per il personale di ambito della CA di Zucchetti le persone a cui può essere assegnato un compito sono individuate tra il personale già assunto secondo le caratteristiche richieste nell'ambito e definite dal responsabile e dal coordinatore dei processi ed in accordo con la funzione aziendale dell'Ufficio Risorse Umane.

5.3.2 Procedure di controllo delle esperienze pregresse

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con l'Ufficio Risorse Umane e un successivo colloquio tecnico con il responsabile di Funzione/Struttura Organizzativa, volto a verificare le skill dichiarate dal candidato. Ulteriori strumenti di verifica sono esercitazioni e test.
Per il personale di ambito della CA di Zucchetti le persone sono individuate secondo quanto definito al punto precedente e su valutazione del Responsabile di CA e del Coordinatore dei processi.

5.3.3 Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, 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 un dipendente Zucchetti ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici, con 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, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

5.3.4 Frequenza di aggiornamento della formazione

Ogni inizio anno viene svolta l'analisi delle esigenze formative propedeutica alla definizione delle attività formative da erogare nell'anno. L'analisi è strutturata nel modo seguente:

- il responsabile segnala alla struttura Zucchetti predisposta (Accademia Zucchetti) la necessità di aggiornamento e formazione;

- Accademia Zucchetti, in considerazione delle esigenze espresse, anche dopo un confronto con la direzione, propone un piano formativo;
- il responsabile approva il piano o richiede modifiche allo stesso;
- in caso di modifiche ripete l'iter sino all'approvazione

5.3.5 Frequenza nella rotazione dei turni di lavoro

n/a

5.3.6 Sanzioni per azioni non autorizzate

Si fa riferimento al "Contratto collettivo nazionale di lavoro aziende del terziario distribuzione e servizi" per la procedura di irrogazione delle sanzioni.

5.3.7 Controlli sul personale non dipendente

n/a

5.3.8 Documentazione che il personale deve fornire

Al momento della selezione, i candidati (potenziali futuri dipendenti) autocertificano i propri dati anagrafici compilando un formulario, l'Ufficio Risorse umane scatta una foto in formato idoneo per l'eventuale successiva predisposizione del badge di accesso ai locali. In fase di selezione le risorse compilano e firmano il consenso al trattamento dei dati personali legati alla selezione; qualora le risorse vengano assunte firmano il consenso al trattamento dei dati personali utile anche al fine della gestione, la lettera di incarico per il trattamento dei dati nonché l'obbligo di riservatezza, impegnandosi a non divulgare notizie e/o documenti riservati.

5.4 Gestione del giornale di controllo

Gli eventi legati alla gestione della CA e della vita del certificato sono raccolti nel giornale di controllo come previsto dal Regolamento e dalle regole tecniche [5].

5.4.1 Tipi di eventi memorizzati

Vengono registrati eventi di sicurezza, avviamento e spegnimento, crash di sistema e guasti hardware, attività di firewall e router e tentativi di accesso sistema PKI.
Vengono conservati tutti i dati e documenti utilizzati in fase di identificazione e accettazione della domanda del richiedente: copia carta d'identità, contrattualistica, visura camerale ecc.
Vengono registrati gli eventi legati alla registrazione e al ciclo di vita dei certificati: le richieste di certificato e rinnovo, le registrazioni del certificato, la generazione, la diffusione, ed eventualmente la revoca/sospensione.
Vengono registrati tutti gli eventi riguardanti le personalizzazioni del dispositivo di firma.
Ogni evento viene salvato con data e ora di sistema dell'evento.

5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo

Il trattamento e raggruppamento dei dati nonché memorizzazione su un sistema di conservazione a norma avviene mensilmente.

5.4.3 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per 20 anni dalla CA.

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita da un sistema di conservazione a norma.

5.4.5 Procedure di backup del giornale di controllo

Il Sistema di Conservazione dei documenti elettronici attua una politica e procedura di backup, come previsto dal manuale della sicurezza del suddetto sistema.

5.4.6 Sistema di memorizzazione del giornale di controllo

La raccolta dei log degli eventi avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dal sistema di conservazione a norma.

5.4.7 Notifica in caso di identificazione di vulnerabilità

n/a

5.4.8 Valutazioni di vulnerabilità

Zucchetti svolge periodicamente delle valutazioni sulle vulnerabilità del Sistema (vulnerability assessment) e test antiintrusione (penetration test). A fronte dei risultati mette in atto tutte le contromisure per mettere in sicurezza le applicazioni

5.5 Archiviazione dei verbali

5.5.1 Tipi di verbali archiviati

Vengono redatti e archiviati verbali relativi ai più importanti eventi di una Certification Authority. I verbali vengono conservati per 20 anni in un sistema di conservazione a norma.

5.5.2 Protezione dei verbali

La protezione è garantita da un Sistema di Conservazione a norma.

5.5.3 Procedure di backup dei verbali

Il sistema di conservazione a norma attua una politica e procedura di backup, come previsto dal manuale della sicurezza del suddetto sistema

5.5.4 Requisiti per la marcatura temporale dei verbali

n/a

5.5.5 Sistema di memorizzazione degli archivi

La raccolta dei verbali avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste da un sistema di conservazione a norma.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

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

5.6 Sostituzione della chiave privata della CA

La CA effettua le procedure di sostituzione periodica della chiave privata di certificazione, utilizzata per la firma dei certificati di sottoscrizione e di quella utilizzata per la firma dei certificati di marcatura temporale, in maniera tale da consentire al Soggetto di poter utilizzare il certificato in suo possesso fino al momento del rinnovo. Ogni sostituzione comporterà una modifica al presente manuale e comunicazione ad Autorità di vigilanza (AgID)

5.7 Compromissione della chiave privata della CA e disaster recovery

5.7.1 Procedure per la gestione degli incidenti

La CA ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27001. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e invio ad AgID della documentazione prevista dall'articolo 19 del Regolamento.

5.7.2 Corruzione delle macchine, del software o dei dati

In caso di guasto del dispositivo sicuro di firma HSM contenente le chiavi di certificazione 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 della CA.

I software e i dati sono soggetti a regolare backup come previsto dalle procedure interne.

5.7.3 Procedure in caso di compromissione della chiave privata della CA

La compromissione della chiave di certificazione è considerato un evento particolarmente critico, in quanto invaliderebbe i certificati emessi firmati con tale chiave. Vi è quindi una particolare attenzione alla protezione della chiave di certificazione e a tutte le attività di sviluppo e manutenzione del sistema che possono avere impatto sulla stessa.
Zucchetti ha descritto la procedura da seguire in caso di compromissione della chiave, nell'ambito del SGSI certificato ISO 27001.

5.7.4 Erogazione dei servizi di CA in caso di disastri

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

5.8 Cessazione del servizio della CA o della RA

Nel caso di cessazione dell'attività di certificazione, Zucchetti comunicherà questa intenzione all'Autorità di vigilanza (AgID) 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 Zucchetti informa della cessazione delle 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 delle attività della CA saranno revocati.

6 CONTROLLI DI SICUREZZA

6.1 Installazione e generazione della coppia di chiavi di certificazione

Per svolgere la sua attività, la Certification Authority ha bisogno di generare la coppia di chiavi di certificazione per la firma dei certificati dei Titolari.

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 e certificati come richiesto dalla normativa vigente.

La protezione delle chiavi private della CA 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. La generazione delle chiavi avviene in presenza del responsabile del servizio.

Le chiavi private della CA 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 e del contesto su più dispositivi come previsto dai criteri di sicurezza del dispositivo HSM.

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'equi probabilità 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.

6.1.1 Generazione della coppia di chiavi del Titolare

Le chiavi asimmetriche sono generate all'interno di un Dispositivo Sicuro per la Creazione della Firma SSCD ovvero QSCD utilizzando le funzionalità native offerte dai dispositivi stessi.
Nel caso in cui il dispositivo non sia messo a diposizione dalla CA, il richiedente deve assicurare che il dispositivo rispetti la normativa vigente, presentando apposita documentazione ed essendo soggetto a audit periodici.

6.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico, sia esso un SSCD o un QSCD. Con la consegna del dispositivo crittografico al Soggetto, questo entra in pieno possesso della chiave privata, che può utilizzare unicamente attraverso l'uso del PIN, di cui ha conoscenza esclusiva.
In caso di processo di registrazione svolto in presenza del Titolare, il dispositivo è consegnato non appena sono generate le chiavi.
In caso di processo di registrazione svolto non in presenza del Soggetto, il dispositivo viene consegnato secondo le modalità condivise nel contratto, avendo sempre cura che il dispositivo e le informazioni per il suo utilizzo viaggino su canali differenti ovvero siano consegnati al Titiolare in due momenti temporalmente differenti.

6.1.3 Consegna della chiave pubblica alla CA

n/a

6.1.4 Consegna della chiave pubblica agli utenti

La chiave pubblica è contenuta nel certificato rilasciato solo al soggetto richiedente. Se il Richiedente

ne fa richiesta, viene pubblicato anche nel registro pubblico, da dove può essere recuperato dall'Utente.

6.1.5 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche di certificazione è generata all'interno di un dispositivo crittografico hardware di cui sopra. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 4096 bit.
Per le chiavi del soggetto l'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è non inferiore a 2048 bit.

6.1.6 Controlli di qualità e generazione della chiave pubblica

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il § 6.2.1) e garantiscono che la chiave pubblica sia corretta e randomica. La CA, prima di emettere il certificato, verifica che la chiave pubblica non sia già stata utilizzata.

6.1.7 Scopo di utilizzo della chiave

Lo scopo di utilizzo della chiave privata è determinato dall'estensione KeyUsage come definita nello standard X509. Per i certificati descritti in questo manuale operativo l'unico utilizzo permesso è "non ripudio", ovvero possono essere utilizzati esclusivamente per firmare.

6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

6.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da Zucchetti per le chiavi di certificazione (CA) e per il risponditore OCSP sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in Europa.
Le smartcard utilizzate da Zucchetti sono validate Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) ovvero EAL5 Augmented by ALC_DVS.2 , AVA_VAN.5 .
I moduli crittografici utilizzati da Zucchetti per le chiavi di firma remota e automatica del Soggetto sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4.

6.2.2 Controllo di più persone della chiave privata di CA

L'accesso ai dispositivi contenenti le chiavi di certificazione avviene solo con due persone autenticate contemporaneamente.

6.2.3 Deposito presso terzi della chiave privata di CA

La chiave privata della CA è depositata presso un QTSP in possesso di tutti i requisiti di qualità e sicurezza che vengono costantemente monitorati.

6.2.4 Backup della chiave privata di CA

Il backup delle chiavi è contenuto in una cassaforte il cui accesso è dato solo al personale che non ha accesso ai dispositivi HSM. Un eventuale ripristino, richiede dunque la presenza sia dl personale che ha accesso ai dispositivi sia di chi ha l'accesso alla cassaforte.

6.2.5 Archiviazione della chiave privata di CA

n/a

6.2.6 Trasferimento della chiave privata da un modulo o su un modulo crittografico

n/a

6.2.7 Memorizzazione della chiave privata su modulo crittografico

La chiave di certificazione viene generata e memorizzata in un'area protetta del dispositivo crittografico che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende bloccato o rende illeggibile il dispositivo stesso

6.2.8 Metodo di attivazione della chiave privata

La chiave privata di certificazione viene attivata dal software della CA in dual control, cioè due persone con ruoli specifici e in presenza del responsabile del servizio.
Il Titolare o il Richiedente legale rappresentante della persona giuridica è responsabile di proteggere la propria chiave privata con una password robusta per prevenire l'utilizzo non autorizzato. Per attivare la chiave privata, il Titolare deve autenticarsi.

6.2.9 Metodo di disattivazione della chiave privata

n/a

6.2.10 Metodo per distruggere la chiave privata della CA

Il personale deputato a questo ruolo si occupa della distruzione della chiave privata quando il certificato è scaduto o revocato, secondo le procedure di sicurezza previste dalle politiche di sicurezza e le specifiche del produttore del dispositivo.

6.2.11 Classificazione dei moduli crittografici

n/a

6.3 Altri aspetti della gestione delle chiavi

n/a

6.3.1 Archiviazione della chiave pubblica

n/a

6.3.2 Periodo di validità del certificato e della coppia di chiavi

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 § 3.3.1.

Attualmente il certificato della CA ha una durata di 12 anni, i certificati emessi a persona fisica hanno validità non superiore ai 3 anni per la firma remota e la business key e non superiore a 5 anni per la firma remota automatica.

6.4 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.2 e 6.3.

6.5 Controlli sulla sicurezza informatica

6.5.1 Requisiti di sicurezza specifici dei computer

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 securizzati (hardening), sono cioè configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della CA.

L'accesso da parte degli Amministratori di sistema, all'uopo nominati in conformità con quanto prescritto dalla normativa vigente, avviene tramite un'applicazione di root on demand che permette l'utilizzo dei privilegi dell'utenza root solo previa autenticazione individuale. Gli accessi sono tracciati e loggati e conservati per 12 mesi.

6.6 Operatività sui sistemi di controllo

Zucchetti attribuisce importanza strategica al trattamento sicuro delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità alla norma ISO/IEC 27001.
Zucchetti è certificata ISO/IEC 27001:2005 da 17 Agosto 2011 per le attività EA:33. L'8 Luglio 2014 è stata certificata per la nuova versione dello standard ISO/IEC 27001:2013.
Nel SGSI sono previsti procedure e controlli per:

- Gestione degli Asset;
- Controllo degli Accessi;
- Sicurezza Fisica ed Ambientale;
- Sicurezza delle Attività Operative;
- Sicurezza delle Comunicazioni;
- Acquisizione, Sviluppo e Manutenzione dei Sistemi;
- Gestione degli Incidenti;
- Continuità Operativa.

Tutte le procedure sono approvate dai relativi responsabili e condivisi internamente nel sistema di gestione documentale Zucchetti.

6.7 Controlli di sicurezza della rete

Per il servizio di certificazione è utilizzata 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.

I sistemi e le reti di Zucchetti sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet,

reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "default deny" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e "defense in depth" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, ed infine l'hardening a livello di sistema).

6.8 Sistema di validazione temporale

Zucchetti fornisce un sistema di validazione temporale qualificato. Per la marcatura temporale fare riferimento al manuale operativo ZUCCHETTI-MO-QTSA presente sul sito del prestatore di servizi fiduciari Zucchetti.

7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP

7.1 Formato del certificato

Nel certificato compaiono le informazioni indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme al Regolamento eiDAS e alla Deliberazione CNIPA [9]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.
Zucchetti utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.
Nell'appendice A il tracciato dei certificati di root e dei titolari.

7.1.1 Numero di versione

Tutti i certificati emessi da Zucchetti sono X.509 versione 3.

7.1.2 Estensioni del certificato

I certificati qualificati sono caratterizzati dalle estensioni presenti nei qcStatement clause 3.2.6 of IETF RFC 3739. Il loro utilizzo è regolato dalla norma ETSI 319 412-5.
Per le estensioni vedere l'appendice A.

7.1.3 OID dell'algoritmo di firma

I certificati sono firmati con il seguente algoritmo:
sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Forme di nomi

Ogni certificato contiene un numero di serie univoco all'interno della CA che lo ha emesso.

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2

7.2 Formato della CRL

Per formare le liste di revoca CRLs, Zucchetti utilizza il profilo RFC5280 "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)" e aggiunge al formato di base le estensioni come definite da RFC 5280: "Authority Key Identifier", "CRL Number", "Issuing Distribution Point" e "expiredCertsOnCRL"

7.2.1 Numero di versione

Tutti le CRL emesse da Zucchetti sono X.509 versione 2.

7.2.2 Estensioni della CRL

Per le estensioni della CRL si veda l'Appendice B.

7.3 Formato dell'OCSP

Zucchetti per determinare lo stato di revoca del certificato senza fare richiesta alla CRL, rende disponibili servizi OCSP conformi al profilo RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". Questo protocollo specifica i dati che devono essere scambiati da un'applicazione che vuole verificare lo stato del certificato e il servizio OCSP.

7.3.1 Numero di versione

Il protocollo OCSP utilizzato da Zucchetti è conforme alla versione 1 del RFC6960.

7.3.2 Estensioni dell'OCSP

Per le estensioni dell'OCSP si veda l'Appendice B.

8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e non, in conformità al Regolamento EIDAS è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento.
Zucchetti ha presentato ad AgID l'apposita richiesta per ottenere il riconoscimento di "prestatore del servizio fiduciario qualificato" allegando un report della valutazione di conformità con il Regolamento (Conformity Assesment Report - CAR) rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.
Zucchetti presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 del 23/07/2014, sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319_403 e UNI CEI EN ISO/IEC 17065:2012.

8.1 Frequenza o circostanze per la valutazione di conformità

La valutazione di conformità viene ripetuta ogni due anni, ma ogni anno il CAB esegue un audit di sorveglianza

8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

Denominazione sociale	**CSQA Certification S.r.l.**
Sede legale	Via S. Gaetano n. 74, 36016 Thiene (VI)
N. di telefono	+39 0445 313011
N. Iscrizione Registro Imprese	Codice Fiscale 02603680246 Registro Imprese VI n. 02603680246 / REA n. 258305
N. partita IVA	02603680246
Sito web	http://www.csqa.it

8.3 Rapporti tra Zucchetti e CAB

Zucchetti e CSQA non hanno interessi finanziari né relazioni di affari.
Non sono in corso rapporti commerciali o di partnership che possono creare pregiudizi a favore o contro Zucchetti nella valutazione obiettiva di CSQA.

8.4 Aspetti oggetto di valutazione

Il CAB è chiamato a valutare la conformità rispetto al Manuale Operativo, al Regolamento e alla normativa applicabile delle procedure adottate, dell'organizzazione della CA, dell'organizzazione dei ruoli, della formazione del personale, della documentazione contrattuale.

8.5 Azioni in caso di non conformità

In caso di non conformità, il CAB deciderà se inviare comunque il rapporto ad AgID, o se riservarsi di rieseguire l'audit dopo che la non conformità sia stata sanata.
Zucchetti si impegna a risolvere tutte le non conformità in maniera tempestiva, mettendo in atto tutte le azioni di miglioramento e adeguamento necessarie.

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

9.1.1 Tariffe per il rilascio e il rinnovo dei certificati

Le tariffe sono disponibili sul sito web all'indirizzo www.firmadigitale.zucchetti.it. La CA può stipulare accordi commerciali con le RA, e/o i Richiedenti prevedendo tariffe specifiche.

9.1.2 Tariffe per l'accesso ai certificati

L'accesso al registro pubblico dei certificati pubblicati è libero e gratuito.

9.1.3 Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati

L'accesso alla lista dei certificati revocati o sospesi è libera e gratuita.

9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili sul sito web all'indirizzo www.firmadigitale.zucchetti.it.

9.1.5 Politiche per il rimborso

Qualora il servizio venga acquistato da un consumatore viene applicata la normativa prevista dal Codice del Consumatore sia per il recesso che per il rimborso.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Zucchetti ha apposita polizza per copertura assicurativa dei rischi derivanti dall'attività descritta in questo manuale per eventuali danni causati a terzi ed il cui testo è stato trattato ed accettato da AgID. Il massimale è di euro 1.000.000 per singolo sinistro e per anno.

9.2.2 Altre attività

n/a

9.2.3 Garanzia o copertura assicurativa per I soggetti finali

Si veda il paragrafo 9.2.1.

9.3 Confidenzialità delle informazioni di business

9.3.1 Ambito di applicazione delle informazioni confidenziali

Nell'ambito dell'attività oggetto del presente Manuale non è prevista la gestione di informazioni confidenziali.

9.3.2 Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali

n/a

9.3.3 Responsabilità di protezione delle informazioni confidenziali

n/a

9.4 Privacy

Le informazioni relative al Titolare e al Richiedente di cui la CA 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 da Zucchetti in conformità a quanto indicato nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018 [4].

9.4.1 Programma sulla privacy

Il programma della privacy è costantemente monitorato e implementato per tener conto della normativa e delle richieste in ambito di certificazione.

9.4.2 Dati che sono trattati come personali

Sono trattati come dati i personali i dati che ricadono nella corrispondente definizione di cui alla normativa vigente [4]; per dato personale si intende quindi qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

9.4.3 Dati non considerati come personali

I dati per i quali è previsto che siano resi pubblici dalla gestione tecnica della CA, ovvero chiave pubblica, certificato (se richiesto dal Titolare), date di revoca e di sospensione del certificato, non sono considerati dati personali.

9.4.4 Titolare del trattamento dei dati personali

Zucchetti S.p.A.
Via Solferino, 1
26900 Lodi LO
Ufficio.privacy@zucchetti.it

9.4.5 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy è disponibile sul sito www.zucchetti.it.
Prima di eseguire ogni trattamento di dati personali, Zucchetti procede a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge [4].

9.4.6 Divulgazione dei dati a seguito di richiesta da parte dell'autorità

La divulgazione di dati su richiesta delle Autorità è obbligatoria e viene svolta nelle modalità stabilite volta per volta dall'Autorità stessa.

9.4.7 Altri motivi di divulgazione

Non previsti.

9.5 Proprietà intellettuale

Il diritto d'autore sul presente documento è di Zucchetti S.p.A. Tutti i diritti sono riservati.

9.6 Rappresentanza e garanzie

Zucchetti mantiene la responsabilità per l'osservazione delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto, ai sensi dell'art. 2.4.1 dell'Allegato al Regolamento di esecuzione UE 2015/1502 della Commissione.
In quest'ultimo caso, la rappresentanza si esplica tramite mandato conferito da Zucchetti all'Ufficio di Registrazione (RA), nel quale vengono definiti il regime di responsabilità e gli obblighi delle parti.
In particolare, l'Ufficio di Registrazione si impegna a svolgere l'attività di registrazione nel rispetto della normativa vigente e delle procedure di cui ai Manuali Operativi, con particolare riferimento all'identificazione personale certa di coloro che sottoscrivono la richiesta di certificazione digitale ed a trasmettere i risultati di tali attività a Zucchetti.
Il Titolare è responsabile della veridicità dei dati comunicati nella Richiesta di Registrazione e Certificazione. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanza indicate nel certificato, sarà considerato responsabile di tutti i danni derivanti al Certificatore e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare il Certificatore da eventuali richieste di risarcimento danni.
Il Titolare e il Richiedente sono altresì responsabili dei danni derivanti al Certificatore e/o a terzi nel caso di ritardo da parte loro dell'attivazione delle procedure previste nel punto 4.9 del presente Manuale (revoca e sospensione del certificato).

9.7 Limitazione di garanzia

Il Certificatore non presta alcuna garanzia sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal Titolare; su usi della chiave privata, del dispositivo sicuro di firma – quando presente – e/o del certificato di sottoscrizione, che siano diversi rispetto a quelli previsti dalle norme vigenti e dal presente Manuale Operativo; sul regolare e continuativo funzionamento di linee e elettriche e telefoniche nazionali e/o internazionali; sulla validità e rilevanza, anche probatoria, del certificato di sottoscrizione o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito, ferma restando l'efficacia di firma autografa riconosciuta alla firma elettronica qualificata, ai sensi dell'art. 25 del Regolamento (UE) n. 910/2014; sulla segretezza e/o integrità di qualsiasi messaggio, atto o documento associato al certificato di sottoscrizione o confezionato tramite le chiavi a cui il certificato è riferito (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili dal Titolare o dal destinatario attraverso l'apposita procedura di verifica).
Il Certificatore garantisce unicamente il funzionamento del Servizio, secondo i livelli indicati al paragrafo 9.17 del Manuale Operativo.

9.8 Limitazione di responsabilità

Il Certificatore non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti e/o, eventualmente, degli hash trasmessi dalla procedura informatica indicata dal Richiedente o dal Titolare, non assumendo alcuna responsabilità, in merito alla validità e riconducibilità degli stessi all'effettiva volontà del Titolare.
Fatto salvo il caso di dolo o colpa, il Certificatore non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificati di sottoscrizione rilasciati in base alle previsioni del presente Manuale e delle "Condizioni generali del servizio di posta elettronica certificata, del servizio di certificazione e del servizio di marcatura temporale",
Zucchetti non è responsabile di qualsiasi danno diretto e/o indiretto derivante in via anche alternativa dalla perdita, dalla impropria conservazione, da un improprio utilizzo, dagli strumenti di identificazione e di autenticazione e/o dalla mancata osservanza di quanto sopra, da parte del Titolare.
Il certificatore, inoltre, fin dalla fase di formazione del Contratto per i servizi di Certificazione, e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e dalla rete internet.
Zucchetti, salvo il caso di dolo o colpa, non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Titolare, al Richiedente e/o a terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati da parte di terzi non autorizzati da Zucchetti.

9.9 Indennizzi

Zucchetti è responsabile degli eventuali danni direttamente determinati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica, in seguito a un mancato adempimento degli obblighi di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo del Consiglio del 23 luglio 2014 e del mancato utilizzo, da parte di Zucchetti, di tutte le misure idonee ad evitare il danno stesso.

Nel caso di cui al paragrafo precedente, il Richiedente o il Titolare avranno diritto di ottenere, a titolo di risarcimento dei danni direttamente subiti in conseguenza del comportamento di cui al paragrafo precedente, un importo che non potrà in ogni caso essere superiore ai valori massimi previsti, per ciascun sinistro e per anno, dall'art. 3, c. 7, del Regolamento allegato alla determinazione 185/2017.

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo improprio del servizio di certificazione o al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili a Zucchetti, quali, a titolo esemplificativo, scioperi, sommosse, terremoti, atti di terrorismo, tumulti popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari hardware e/o dei software utilizzati dal Richiedente.

9.10 Termine e risoluzione

9.10.1 Termine

Al termine del rapporto tra CA e Titolare, tra CA e RA, tra CA e Richiedente, il certificato viene revocato.

9.10.2 Risoluzione

Si rimanda alla contrattualistica che regolamenta il servizio per il dettaglio delle modalità di

risoluzione del contratto.

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata revoca del certificato.

9.11 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1.

9.12 Revisione del Manuale Operativo

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

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo Manuale Operativo verrà prontamente comunicata alle RA.
Se i cambiamenti sono rilevanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (CAR – Conformity Assessment Report) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

Versione/Release n°:	2.1	**Data Versione/Release**:	07/05/18
Descrizione modifiche:	3.1.5 Riscrittura parziale paragrafo per migliore comprensibilità 3.2.3 Riscrittura parziale paragrafo per migliore comprensibilità 4.2.1 Riscrittura parziale paragrafo per migliore comprensibilità 9.4 Aggiunta riferimenti al GDPR 9.6, 9.7, 9.8 e 9.9 Dettagliati maggiormente i paragrafi Correzione refusi		
Motivazioni:	Aggiornato per adeguamento alla nuova normativa privacy		

Versione/Release n°:	2.0	**Data Versione/Release**:	22/05/17
Descrizione modifiche:	Adeguamento alla struttura prevista da IETF RFC 3647		
Motivazioni:	Aggiornato per adempimento normativa EIDAS		

9.12.1 Storia delle revisioni

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

Versione/Release n°:	1.4	**Data Versione/Release**:	21/11/16
Descrizione modifiche:	Rilascio telematico, disponibilità servizio		
Motivazioni:	Quinta 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°:	1.2	**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°:	1.1	**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°:	1.0	**Data Versione/Release**:	20/07/15
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

9.12.2 Procedure di revisione

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le revisioni sono apportate di concerto con il Responsabile del Servizio di Certificazione, il Responsabile della Privacy e l'Ufficio Legale e approvate dal management.

9.12.3 Periodo e maccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del TSP (indirizzo: www.firmadigitale.zucchetti.it);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;
- in formato cartaceo può essere richiesto alle Registration Authority o al contatto per gli utenti finali.

9.12.4 Casi nei quali l'OID deve cambiare

n/a

9.13 Risoluzione delle controversie

Si rimanda alla contrattualistica che regolamenta il servizio per il dettaglio delle modalità di risoluzione delle controversie.

9.14 Foro competente

Per i consumatori il foro competente è il tribunale della città dove il consumatore ha il domicilio. Per i soggetti diversi dai consumatori, il foro competente è quello di Lodi. Negli accordi tra CA e RA, tra CA e Richiedente o tra CA e Titolare può essere definito un diverso foro competente.

9.15 Legge applicabile

La legge applicabile al presente Manuale Operativo è la legge italiana.

Di seguito un elenco non esaustivo dei principali riferimenti normativi applicabili:

[1] 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 (referenziato anche come Regolamento eIDAS)
[2] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (referenziato anche come CAD) e ss.m.ii.
[3] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e ss.mm.ii
[4] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018).
[5] DPCM 22 febbraio 2013 (GU n.117 del 21-5-2013) - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.
[6] D.Lgs. 21 novembre 2007, n. 231 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e ss.mm.ii
[7] non utilizzato
[8] non utilizzato
[9] Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determine successive

[10] Determinazione AgID n°189/2017

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza[5], nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].

9.16 Disposizioni varie

Si rimanda alla contrattualistica che regolamenta il servizio per ogni altra disposizione non compresa nel presente Manuale.

9.17 Altre disposizioni

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

(*) 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.

[5] Disponibili sul sito http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

APPENDICE A - ROOT CA

```
0 1238: SEQUENCE {
   4  958:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
         :       }
  13    1:     INTEGER 5
  16   13:     SEQUENCE {
  18    9:       OBJECT IDENTIFIER
         :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
  29    0:       NULL
         :       }
  31  135:     SEQUENCE {
  34   11:       SET {
  36    9:         SEQUENCE {
  38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  43    2:           PrintableString 'IT'
         :           }
         :         }
  47   25:       SET {
  49   23:         SEQUENCE {
  51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
  56   16:           UTF8String 'Zucchetti S.p.A.'
         :           }
         :         }
  74   34:       SET {
  76   32:         SEQUENCE {
  78    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
  83   25:           UTF8String 'Certificatore Accreditato'
         :           }
         :         }
 110   19:       SET {
 112   17:         SEQUENCE {
 114    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
 119   10:           PrintableString '5006900962'
         :           }
         :         }
 131   36:       SET {
 133   34:         SEQUENCE {
 135    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 140   27:           UTF8String 'Zucchetti Firma Qualificata'
         :           }
         :         }
         :       }
 169   30:     SEQUENCE {
 171   13:       UTCTime 05/11/2015 10:51:34 GMT
 186   13:       UTCTime 05/11/2027 11:51:34 GMT
         :       }
 201  135:     SEQUENCE {
 204   11:       SET {
 206    9:         SEQUENCE {
 208    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 213    2:           PrintableString 'IT'
```

```
        :           }
        :         }
 217   25:       SET {
 219   23:         SEQUENCE {
 221    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 226   16:           UTF8String 'Zucchetti S.p.A.'
        :           }
        :         }
 244   34:       SET {
 246   32:         SEQUENCE {
 248    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 253   25:           UTF8String 'Certificatore Accreditato'
        :           }
        :         }
 280   19:       SET {
 282   17:         SEQUENCE {
 284    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
 289   10:           PrintableString '5006900962'
        :           }
        :         }
 301   36:       SET {
 303   34:         SEQUENCE {
 305    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 310   27:           UTF8String 'Zucchetti Firma Qualificata'
        :           }
        :         }
        :       }
 339  290:     SEQUENCE {
 343   13:       SEQUENCE {
 345    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
 356    0:         NULL
        :         }
 358  271:       BIT STRING, encapsulates {
 363  266:         SEQUENCE {
 367  257:           INTEGER
        :             00 85 9F 8C F2 34 C8 6E 25 DC 27 A8 AF 35 E0 12
        :             76 74 9B D8 E1 E6 DB 98 16 CA EE 12 47 7B F0 2B
        :             10 6C 17 CD 89 BF 96 3D EA 52 D5 B1 49 F4 7F 83
        :             13 73 02 0D B2 74 70 5E C2 4B C8 48 CF 49 34 45
        :             4A 21 6C 03 5E E4 EE 77 C7 6F DE 01 8B DD 6C 82
        :             01 BC 15 3C 83 F9 D6 9A 98 2E F3 74 92 DA FA C5
        :             2A 5E B8 68 14 A9 9F EC A2 7B 05 8A 30 76 4A B1
        :             F0 9D 74 E5 F7 8A 8F E0 AE AD B0 E1 92 C7 BC E0
        :                     [ Another 129 bytes skipped ]
 628    3:           INTEGER 65537
        :           }
        :         }
        :       }
 633  329:     [3] {
 637  325:       SEQUENCE {
 641   15:         SEQUENCE {
 643    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 648    1:           BOOLEAN TRUE
 651    5:           OCTET STRING, encapsulates {
 653    3:             SEQUENCE {
 655    1:               BOOLEAN TRUE
        :               }
        :             }
```

```
        :           }
 658   64:         SEQUENCE {
 660    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 665   57:           OCTET STRING, encapsulates {
 667   55:             SEQUENCE {
 669   53:               SEQUENCE {
 671    4:                 OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 677   45:                 SEQUENCE {
 679   43:                   SEQUENCE {
 681    8:                     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
 691   31:                     IA5String 'https://ca.zucchetti.it/doc/mo/'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
 724  192:         SEQUENCE {
 727    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
 732  184:           OCTET STRING, encapsulates {
 735  181:             SEQUENCE {
 738  178:               SEQUENCE {
 741  175:                 [0] {
 744  172:                   [0] {
 747   53:                     [6]
        :
'http://crl.ca.zucchetti.it/FirmaQualificata/CACR'
        :                     'L.crl'
 802  115:                     [6]
        :
'ldap://ldap.ca.zucchetti.it/cn%3DZucchetti%20Fir'
        :
'ma%20Qualificata,o%3DZucchetti%20SpA,c%3DIT?auth'
        :                     'orityRevocationList'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
 919   14:         SEQUENCE {
 921    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
 926    1:           BOOLEAN TRUE
 929    4:           OCTET STRING, encapsulates {
 931    2:             BIT STRING 1 unused bit
        :               '1100000'B
        :             }
        :           }
 935   29:         SEQUENCE {
 937    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
 942   22:           OCTET STRING, encapsulates {
 944   20:             OCTET STRING
        :               10 9C F6 CB 93 B6 EA C4 E9 F4 92 D9 61 AC FE D0
        :               B3 85 FD 33
        :             }
        :           }
        :         }
        :       }
```

```
         :     }
 966   13:   SEQUENCE {
 968    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1
1 11)
 979    0:     NULL
         :     }
 981  257:   BIT STRING
         :     19 AD DC F6 38 AA 81 61 25 62 93 6C BA 8A 26 66
         :     36 68 D2 82 80 DF B9 AB DB 45 57 D0 5B CA B2 B2
         :     7C FD 0A B9 3D 29 90 82 F8 DE 9B 5B 52 B2 61 B3
         :     86 52 1D 1E F3 61 43 61 3A 3D 59 D7 50 47 A4 EA
         :     4E 91 DD 58 E8 51 96 18 9B 32 37 23 14 18 81 03
         :     68 9A 73 0C 56 F4 60 85 32 D8 36 D5 E6 54 71 BC
         :     0C 53 F9 5C C2 C5 84 D1 A4 B4 3F 62 FD B5 A4 01
         :     9D 1C 49 2B 1B 99 18 CC 83 AA 6A 34 20 A6 5D A9
         :             [ Another 128 bytes skipped ]
         :   }
```

Certificato qualificato persona fisica SENZA identificatori di semantica e chiavi su QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	Zucchetti S.p.A.
Organizational Unit Name:	Certificatore Accreditato
Organization Identifier:	5006900962
Common Name:	Zucchetti Firma Qualificata
VALIDITY:	3 or 5 years ***(****)***
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence) (*****)*
Organization Identifier:	*(conditioned presence)* ***(***)***
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)*** *as defined clause 5.1.3 of ETSI en 319 412-1 (i.e. "TINIT-CodiceFiscale", "PASIT-PassportNumber", "IDCIT - IdentityCardNumber")*
Pseudonym:	*(conditioned presence)* ***(*)***
Title	*Holder's specific qualification (optional)*
Locality	*(conditioned presence) (******)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	

Uniform Resource ID1:	
http://crl.ca.zucchetti.it/FirmaQualificata/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.ca.zucchetti.it/cn%3DZucchetti%20Firma%20Qualificata%20CRL**xx**,o%3DZucchetti%20SpA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.zucchetti.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	https://cert.ca.zucchetti.it/ca/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.45.1.1.1 • 1.3.76.45.1.1.2 • 1.3.76.45.1.1.4
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	https://ca.zucchetti.it/doc/mo/
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*

ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE (optional)*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****):** in case of automatic signature (OID* 1.3.76.45.1.1.2 *) is 5 years.*	
(*****): if the organization attribute is present, contains more information about the organization itself. This attribute may appear, at most, four times.	
(******): if the organization attribute is present, contains information relevant to the specified organization.	
NB: xx = partitioned revocation list progressive numbering	

APPENDICE B - FORMATO DELLE CRL E OCSP

Estensione	Valore
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	CN = Zucchetti Firma Qualificata SERIALNUMBER = 5006900962 OU = Certificatore Accreditato O = Zucchetti S.p.A. C = IT
thisUpdate	Data in formato UTC
nextUpdate	Data della prossima CRL In format
Revoked Certificates List	Lista dei certificati revocati, con numero di serie e data di revoca/sospensione
Issuer's Signature	Firma della CA

Valori ed estensioni per CRL e OCSP

Le CRL hanno le seguenti estensioni

Extension	Value
Authority Key Identifier	Il valore dell'impronta 160-bit SHA-1 di issuerPublicKey
CRL number	Il numero univoco della CRL assegnato dalla CA
ExpiredCertsOnCRL	La data in formato GeneralizedTime dalla quale i certificati scaduti sono tenuti in CRL. Il valore è impostato uguale alla data di emissione della CA
Issuing Distribution Point	Identifica il punto di distribuzione delle CRL e lo scopo: indica se la CRL è generata solo per certificati di CA o del soggetto (end-entity)
Invalidity Date	Data in formato UTC che indica la data da cui si ritiene che il certificate sia invalido

La richiesta OCSP contiene i seguenti campi:

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash del DN dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente.
Serial Number	Numero di serie del certificato

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	Stato della risposta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificato firmatario della risposta OCSP.
Produced at	Data in formato GeneralizedTime di quando è stata generate la

	risposta OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash del distinguishName dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente
Serial Number	Numero di serie del certificato
thisUpdate	La data di verifica dello stato del certificato in formato GeneralizedTime
nextUpdate	Data in cui lo stato del certificato potrebbe essere aggiornato
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

OCSP Extensions

La richiesta OCSP può contenere le seguenti estensioni:

Extension	Value
nonce	Un numero arbitrario che può essere usato una sola volta. Crittograficamente lega una richiesta alla sua risposta per prevenire attacchi da replica. E' contenuto in una una requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in una responseExtensions.

APPENDICE C - STRUMENTI E MODALITÀ PER L'APPOSIZIONE E LA VERIFICA DELLA FIRMA DIGITALE

Zucchetti mette a disposizione un prodotto (denominato "FirmaCheck") gratuitamente scaricabile dai Titolari dal sito www.firmadigitale.zucchetti.it per consentire:

- di firmare digitalmente documenti a tutti i Soggetti in possesso di un certificato emesso da Zucchetti;
- la verifica della firma apposta a documenti firmati digitalmente secondo i formati definiti dalle Regole Tecniche [5] e dalla Deliberazione CNIPA [9].

Gli ambienti in cui FirmaCheck opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo web sopra indicato. Le istruzioni per l'utilizzo del prodotto sono incluse nel prodotto stesso e consultabili tramite la funzione di help. Nel documento denominato "Manuale d'uso FirmaCheck", sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale. Il prodotto FirmaCheck è in grado di firmare qualsiasi tipo di file. La possibilità di visualizzare il file dipende dalla disponibilità sulla stazione di lavoro dell'utente di un adeguato software di visualizzazione.

Zucchetti può mettere a disposizione, a pagamento e secondo gli accordi commerciali tempo per tempo stabiliti con le RA, i Richiedenti, i Titolari o gli Utenti, ulteriori prodotti o servizi di firma e/o di verifica della firma, nel rispetto delle Regole Tecniche [5] e della Deliberazione CNIPA [9].

I documenti elettronici sottoscritti con certificati emessi da Zucchetti possono essere verificati anche attraverso altri strumenti, in grado di interpretare i formati di firma previsti. Tali strumenti sono fuori dalla responsabilità di Zucchetti[6].

Avvertenza

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 25 comma 2 del Regolamento [1], ossia non può considerarsi equivalente rispetto a una firma autografa. È cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.

[6] Ad esempio, la verifica di una firma in formato conforme allo standard PadES (PDF Advanced Electronic Signatures) può essere effettuata utilizzando il software Adobe Reader scaricabile gratuitamente dal sito www.adobe.com/it.