

Zucchetti

Autorità di Certificazione

Certificati di Sottoscrizione – Firma Elettronica Avanzata
Manuale Operativo

ZUCCHETTI-MO-FEA

Questa pagina è lasciata
intenzionalmente bianca

Indice

1	INTRODUZIONE	10
1.1	Quadro Generale	10
1.2	Nome e identificativo del documento	10
1.3	Partecipanti e responsabilità.....	11
1.3.1	Certification Authority – Autorità di Certificazione	11
1.3.2	Registration authority – Ufficio di Registrazione (RA)	11
1.3.2.1	Incaricato alla Registrazione (IR).....	11
1.3.3	Titolare	12
1.3.4	Utente	12
1.3.5	Richiedente.....	12
1.3.6	Autorità.....	12
1.3.6.1	Agenzia per l’Italia Digitale - AgID.....	12
1.3.6.2	Organismo di valutazione della conformità - Conformity Assessment Body	12
1.4	Uso del certificato	12
1.4.1	Usi consentiti.....	12
1.4.2	Usi non consentiti.....	13
1.5	Amministrazione del Manuale Operativo	13
1.5.1	Contatti	13
1.5.2	Soggetti responsabili dell’approvazione del Manuale Operativo	13
1.5.3	Procedure di approvazione	13
1.6	Definizioni e acronimi.....	13
1.6.1	Definizioni.....	13
1.6.2	Acronimi e abbreviazioni	16
2	PUBBLICAZIONE E ARCHIVIAZIONE	18
2.1	Archiviazione	18
2.2	Pubblicazione delle informazioni sulla certificazione	18
2.2.1	Pubblicazione del manuale operativo.....	18
2.2.2	Pubblicazione dei certificati	18
2.2.3	Pubblicazione delle liste di revoca	18
2.3	Periodo o frequenza di pubblicazione	18
2.3.1	Frequenza di pubblicazione del manuale operativo	18
2.3.2	Frequenza pubblicazione delle liste di revoca.....	18
2.4	Controllo degli accessi agli archivi pubblici	18
3	IDENTIFICAZIONE E AUTENTICAZIONE.....	19
3.1	Denominazione.....	19
3.1.1	Tipi di nomi.....	19
3.1.2	Necessità che il nome abbia un significato	19
3.1.3	Anonimato e pseudonimia dei richiedenti.....	19
3.1.4	Regole di interpretazione dei tipi di nomi.....	19
3.1.5	Univocità dei nomi	19

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

3.1.6	Riconoscimento, autenticazione e ruolo dei marchi registrati	19
3.2	Convalida iniziale dell'identità	19
3.2.1	Metodo per dimostrare il possesso della chiave privata.....	20
3.2.2	Autenticazione dell'identità delle organizzazioni	20
3.2.3	Identificazione della persona fisica	20
3.2.3.1	Riconoscimento effettuato secondo la modalità 1 – De Visu.....	20
3.2.3.2	Riconoscimento effettuato secondo la modalità 2 – VideoID	21
3.2.3.3	Riconoscimento effettuato secondo la modalità 3 – SPID	21
3.2.3.4	Riconoscimento effettuato secondo la modalità 4 – CIE.....	21
3.2.4	Identificazione della persona giuridica	21
3.2.5	Informazioni del Titolare o del Richiedente non verificate	22
3.2.6	Validazione dell'autorità	22
3.3	Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati.....	22
3.3.1	Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati.....	22
3.4	Identificazione e autenticazione per le richieste di revoca.....	22
3.4.1	Richiesta da parte del Titolare.....	22
3.4.2	Richiesta da parte del Richiedente	22
4	OPERATIVITÀ.....	23
4.1	Richiesta del certificato	23
4.1.1	Chi può richiedere un certificato	23
4.1.2	Processo di registrazione e responsabilità.....	23
4.2	Elaborazione della richiesta	23
4.2.1	Informazioni che il Titolare deve fornire	23
4.2.2	Esecuzione delle funzioni di identificazione e autenticazione.....	24
4.2.3	Approvazione o rifiuto della richiesta del certificato.....	24
4.2.4	Tempo massimo per l'elaborazione della richiesta del certificato.....	24
4.3	Emissione del certificato	24
4.3.1	Azioni della CA durante l'emissione del certificato	24
4.3.2	Notifica ai richiedenti dell'avvenuta emissione del certificato	24
4.3.3	Attivazione	24
4.4	Accettazione del certificato	24
4.4.1	Comportamenti concludenti di accettazione del certificato	24
4.4.2	Pubblicazione del certificato da parte della Certification Authority.....	25
4.4.3	Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato.....	25
4.5	Uso della coppia di chiavi e del certificato	25
4.5.1	Uso della chiave privata e del certificato da parte del Titolare.....	25
4.5.2	Uso della chiave pubblica e del certificato da parte degli Utenti Finali	25
4.5.3	Limiti d'uso e di valore	25
4.6	Rinnovo del certificato	25
4.6.1	Motivi per il rinnovo	25
4.6.2	Chi può richiedere il rinnovo	26
4.6.3	Elaborazione della richiesta di rinnovo del certificato.....	26
4.7	Riemissione del certificato	26
4.8	Modifica del certificato	26
4.9	Revoca del certificato.....	26
4.9.1	Motivi per la revoca	26
4.9.2	Chi può richiedere la revoca.....	26

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

4.9.3	Procedure per richiedere la revoca	26
4.9.3.1	Revoca richiesta dal Titolare	27
4.9.3.2	Revoca su iniziativa della Certification Authority	27
4.9.4	Periodo di grazia della richiesta di revoca	27
4.9.5	Tempo massimo di elaborazione della richiesta di revoca.....	27
4.9.6	Requisiti per la verifica della revoca.....	27
4.9.7	Frequenza di pubblicazione della CRL	27
4.9.8	Latenza massima della CRL.....	28
4.9.9	Servizi online di verifica dello stato di revoca del certificato.....	28
4.9.10	Requisiti servizi on line di verifica	28
4.9.11	Altre forme di revoca	28
4.9.12	Requisiti specifici rekey in caso di compromissione	28
4.9.13	Motivi per la sospensione.....	28
4.9.14	Chi può richiedere la sospensione	28
4.9.15	Procedure per richiedere la sospensione	28
4.9.16	Limiti al periodo di sospensione	28
4.10	Servizi riguardanti lo stato del certificato	28
4.10.1	Caratteristiche operative.....	28
4.10.2	Disponibilità del servizio	28
4.10.3	Caratteristiche opzionali.....	29
4.11	Disdetta dai servizi della CA.....	29
4.12	Deposito presso terzi e recovery della chiave	29
5	MISURE DI SICUREZZA E CONTROLLI	30
5.1	Sicurezza fisica.....	30
5.1.1	Posizione e costruzione della struttura	30
5.1.2	Accesso fisico.....	31
5.1.3	Impianto elettrico e di climatizzazione	31
5.1.3.1	Data Center Siziano.....	31
5.1.3.2	Data Center Padova.....	32
5.1.4	Prevenzione e protezione contro gli allagamenti	32
5.1.4.1	Data Center Siziano.....	32
5.1.4.2	Data Center Padova.....	32
5.1.5	Prevenzione e protezione contro gli incendi	33
5.1.5.1	Data Center Siziano.....	33
5.1.5.2	Data Center Padova.....	33
5.1.6	Supporti di memorizzazione.....	33
5.1.6.1	Data Center Siziano.....	33
5.1.6.2	Data Center Padova.....	33
5.1.7	Smaltimento dei rifiuti	33
5.1.7.1	Data Center Siziano.....	33
5.1.7.2	Data Center Padova.....	34
5.1.8	Off-site backup	34
5.1.8.1	Data Center Siziano.....	34
5.1.8.2	Data Center Padova.....	34
5.2	Controlli procedurali	34
5.2.1	Ruoli chiave.....	34
5.3	Controllo del personale	34
5.3.1	Qualifiche, esperienze e autorizzazioni richieste	34
5.3.2	Procedure di controllo delle esperienze pregresse	34

5.3.3	Requisiti di formazione	35
5.3.4	Frequenza di aggiornamento della formazione	35
5.3.5	Frequenza nella rotazione dei turni di lavoro	35
5.3.6	Sanzioni per azioni non autorizzate	35
5.3.7	Controlli sul personale non dipendente	35
5.3.8	Documentazione che il personale deve fornire	35
5.4	Gestione del giornale di controllo	35
5.4.1	Tipi di eventi memorizzati	35
5.4.2	Frequenza di trattamento e di memorizzazione del giornale di controllo	36
5.4.3	Periodo di conservazione del giornale di controllo	36
5.4.4	Protezione del giornale di controllo	36
5.4.5	Procedure di backup del giornale di controllo	36
5.4.6	Sistema di memorizzazione del giornale di controllo	36
5.4.7	Notifica in caso di identificazione di vulnerabilità	36
5.4.8	Valutazioni di vulnerabilità	36
5.5	Archiviazione dei verbali	36
5.5.1	Tipi di verbali archiviati	36
5.5.2	Protezione dei verbali	36
5.5.3	Procedure di backup dei verbali	37
5.5.4	Requisiti per la marcatura temporale dei verbali	37
5.5.5	Sistema di memorizzazione degli archivi	37
5.5.6	Procedure per ottenere e verificare le informazioni contenute negli archivi	37
5.6	Sostituzione della chiave privata della CA	37
5.7	Compromissione della chiave privata della CA e disaster recovery	37
5.7.1	Procedure per la gestione degli incidenti	37
5.7.2	Corruzione delle macchine, del software o dei dati	37
5.7.3	Procedure in caso di compromissione della chiave privata della CA	37
5.7.4	Erogazione dei servizi di CA in caso di disastri	38
5.8	Cessazione del servizio della CA o della RA	38
6	CONTROLLI DI SICUREZZA	39
6.1	Installazione e generazione della coppia di chiavi di certificazione	39
6.1.1	Generazione della coppia di chiavi del Titolare	39
6.1.2	Consegna della chiave privata al Richiedente	39
6.1.3	Consegna della chiave pubblica alla CA	39
6.1.4	Consegna della chiave pubblica agli utenti	39
6.1.5	Algoritmo e lunghezza delle chiavi	39
6.1.6	Controlli di qualità e generazione della chiave pubblica	40
6.1.7	Scopo di utilizzo della chiave	40
6.1.7.1	Utilizzo chiave di CA	40
6.1.7.2	Utilizzo chiave del Soggetto	40
6.2	Protezione della chiave privata e controlli ingegneristici del modulo crittografico 40	
6.2.1	Controlli e standard del modulo crittografico	40
6.2.2	Controllo di più persone della chiave privata di CA	40
6.2.3	Deposito presso terzi della chiave privata di CA	40
6.2.4	Backup della chiave privata di CA	41
6.2.5	Archiviazione della chiave privata di CA	41

6.2.6	Trasferimento della chiave privata da un modulo o su un modulo crittografico	41
6.2.7	Memorizzazione della chiave privata su modulo crittografico	41
6.2.8	Metodo di attivazione della chiave privata	41
6.2.9	Metodo di disattivazione della chiave privata	41
6.2.10	Metodo per distruggere la chiave privata della CA	41
6.2.11	Classificazione dei moduli crittografici	41
6.3	Altri aspetti della gestione delle chiavi	41
6.3.1	Archiviazione della chiave pubblica	41
6.3.2	Periodo di validità del certificato e della coppia di chiavi	41
6.4	Dati di attivazione della chiave privata	42
6.5	Controlli sulla sicurezza informatica	42
6.5.1	Requisiti di sicurezza specifici dei computer	42
6.6	Operatività sui sistemi di controllo	42
6.7	Controlli di sicurezza della rete	43
6.8	Sistema di validazione temporale	43
7	FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP	44
7.1	Formato del certificato	44
7.1.1	Numero di versione	44
7.1.2	Estensioni del certificato	44
7.1.3	OID dell'algoritmo di firma	44
7.1.4	Forme di nomi	44
7.1.5	Vincoli ai nomi	44
7.1.6	OID del certificato	44
7.2	Formato della CRL	44
7.2.1	Numero di versione	44
7.2.2	Estensioni della CRL	44
7.3	Formato dell'OCSP	45
7.3.1	Numero di versione	45
7.3.2	Estensioni dell'OCSP	45
8	CONTROLLI E VALUTAZIONI DI CONFORMITÀ	46
8.1	Frequenza o circostanze per la valutazione di conformità	46
8.2	Identità e qualifiche di chi effettua il controllo	46
8.3	Rapporti tra Zucchetti e CAB	46
8.4	Aspetti oggetto di valutazione	46
8.5	Azioni in caso di non conformità	46
9	ALTRI ASPETTI LEGALI E DI BUSINESS	47
9.1	Tariffe	47
9.1.1	Tariffe per il rilascio e il rinnovo dei certificati	47
9.1.2	Tariffe per l'accesso ai certificati	47
9.1.3	Tariffe per l'accesso alle informazioni sullo stato di revoca dei certificati	47
9.1.4	Tariffe per altri servizi	47
9.1.5	Politiche per il rimborso	47
9.2	Responsabilità finanziaria	47
9.2.1	Copertura assicurativa	47
9.2.2	Altre attività	47

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

9.2.3	Garanzia o copertura assicurativa per i soggetti finali	47
9.3	Confidenzialità delle informazioni di business	47
9.3.1	Ambito di applicazione delle informazioni confidenziali	47
9.3.2	Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali	48
9.3.3	Responsabilità di protezione delle informazioni confidenziali	48
9.4	Privacy.....	48
9.4.1	Programma sulla privacy.....	48
9.4.2	Dati che sono trattati come personali	48
9.4.3	Dati non considerati come personali	48
9.4.4	Titolare del trattamento dei dati personali.....	48
9.4.5	Informativa privacy e consenso al trattamento dei dati personali	48
9.4.6	Divulgazione dei dati a seguito di richiesta da parte dell'autorità	48
9.4.7	Altri motivi di divulgazione	49
9.5	Proprietà intellettuale	49
9.6	Rappresentanza e garanzie	49
9.7	Limitazione di garanzia	49
9.8	Limitazione di responsabilità	49
9.9	Indennizzi	50
9.10	Termine e risoluzione.....	50
9.10.1	Termine	50
9.10.2	Risoluzione.....	50
9.10.3	Effetti della risoluzione	50
9.11	Canali di comunicazione ufficiali	51
9.12	Revisione del Manuale Operativo	51
9.12.1	Storia delle revisioni.....	51
9.12.2	Procedure di revisione	51
9.12.3	Periodo e meccanismo di notifica	52
9.12.4	Casi nei quali l'OID deve cambiare	52
9.13	Risoluzione delle controversie	52
9.14	Foro competente	52
9.15	Legge applicabile	52
9.16	Disposizioni varie.....	53
9.17	Altre disposizioni	53
APPENDICE A - ROOT CA.....		54
	Certificato di root CA Zucchetti Advanced Electronic Signature CA 2	54
	Certificato titolare Zucchetti Advanced Electronic Signature CA 2.....	62
	Certificato titolare Zucchetti Advanced Electronic Signature CA 2.....	64
APPENDICE B - FORMATO DELLE CRL E OCSP		66
	Valori ed estensioni per CRL e OCSP	66
	OCSP Extensions	68

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 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, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, e in generale di tutto ciò che rende affidabile un certificato in conformità con la vigente normativa in materia di servizi fiduciari in particolare di firma elettronica avanzata. 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 Firma Elettronica Avanzata – Manuale Operativo" ed è caratterizzato dal codice documento: **ZUCCHETTI-MO-FEA**.

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 è il seguente:

L'*object identifier* (OID) che identifica Zucchetti è 1.3.76.45

Le policy per certificati qualificati su dispositivo qualificato sono:

Manuale-operativo-certificato di tipo one-shot 24 ore emesso a persona fisica con chiavi RSA su dispositivo	1.3.76.45.1.1.8 conforme alla policy NCP+
Manuale-operativo-certificato di tipo one-shot 72 ore emesso a persona fisica con chiavi RSA su dispositivo	1.3.76.45.1.1.9 conforme alla policy NCP+
Manuale-operativo-certificato di tipo one-shot 24 ore emesso a persona fisica con chiavi EC su dispositivo	1.3.76.45.1.1.11 conforme alla policy NCP+

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo 4.5.3. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del Manuale Operativo.

Questo documento è pubblicato in formato elettronico presso il sito Web del Certificatore all'indirizzo www.zuccheticertifica.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 di firma, 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, 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	Piazza Mino Zucchetti, 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.zucchetticertifica.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,
- 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 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.

1.3.2.1 Incaricato alla Registrazione (IR)

La CA e la RA possono 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 tramite apposite indicazioni fornite 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, 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 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 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.

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 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 e dei servizi fiduciari 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 per la firma elettronica avanzata ai sensi del CAD [1] e dell'articolo 26 del Regolamento Eidas [1].

Il certificato emesso dalla CA sarà usato per verificare la firma elettronica avanzata del Titolare cui il certificato appartiene.

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
Piazza Mino Zucchetti, 1
26900 Lodi

Web: www.zucchetticertifica.it

e-mail: signbook@zucchetti.it

Il Titolare può richiedere copia della documentazione a lui relativa, inoltrando apposita richiesta all'indirizzo signbook@zucchetti.it.

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.

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.

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

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])
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])
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])
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 soddisfa i requisiti di cui all'articolo 26 del Regolamento eIDAS (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]).

Certificati di Sottoscrizione

Manuale Operativo ZUCCHETTI-MO-FEA

Termine	Definizione
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])
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: <ul style="list-style-type: none"> ▪ 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: <ol style="list-style-type: none"> 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])
Tempo Universale Coordinato [Coordinated Universal Time]:	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.

Certificati di Sottoscrizione Manuale Operativo ZUCCHETTI-MO-FEA

Termine	Definizione
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])

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
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;

Certificati di Sottoscrizione Manuale Operativo ZUCCHETTI-MO-FEA

Acronimo	
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
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: Rivest, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SPID	Sistema Pubblico di Identità Digitale
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. § 1.3.1)

2.2.2 Pubblicazione dei certificati

Non è prevista la pubblicazione

2.2.3 Pubblicazione delle liste di revoca

Le liste di revoca sono pubblicate nel registro pubblico dei certificati accessibile con protocollo HTTP. L'indirizzo (URL) 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 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.

2.3.2 Frequenza pubblicazione delle liste di revoca

Le CRLs vengono pubblicate ogni ora.

2.4 Controllo degli accessi agli archivi pubblici

Le informazioni relative 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 in conformità con quanto stabilito nella specifica RFC-5280.

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, a seguito di analisi sulla fattibilità, un codice identificativo tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento. Il formato è quello previsto dallo std ETSI 319 412-1.

Tuttavia, essendo il codice fiscale utilizzato da tutte le amministrazioni pubbliche italiane come identificativo del cittadino e del contribuente, la sua mancata indicazione all'interno del certificato di firma, comporta l'inadeguatezza dello stesso verso la Pubblica Amministrazione italiana.

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, pertanto il Titolare e il Richiedente si assumono la piena responsabilità in merito all'utilizzo di marchi registrati all'interno del certificato.

La CA può inoltre rifiutarsi di generare o può richiedere 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.

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	<ul style="list-style-type: none">• Certification Authority (CA)• Registration Authority (RA)• Incaricato alla Registrazione	n/a
2 VideoID	<ul style="list-style-type: none">• Certification Authority (CA)• Registration Authority (RA)• Incaricato alla Registrazione	n/a
3 SPID	<ul style="list-style-type: none">• Certification Authority (CA)• Registration Authority (RA)• Incaricato alla Registrazione	Utilizzo di identità rilasciate nel contesto del sistema SPID
4 CIE	<ul style="list-style-type: none">• Certification Authority (CA)• Registration Authority (RA)• Incaricato alla Registrazione	Utilizzo della CIE

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 validità¹. Per garantire l'univocità del Titolare e del relativo nome, questi deve essere in

¹ Per i titolari di firma con cittadinanza italiana vengono accettati i seguenti documenti:

- carta d'identità
- patente di guida
- passaporto

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).

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.

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 – VideoID

Nella modalità **VideoID** è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphone, tablet, etc.), una webcam e un sistema audio funzionante.

Il Soggetto o il Richiedente, in una prima fase, invieranno le evidenze a supporto della verifica dell'identità attraverso la compilazione di un'apposita form che prevede l'inserimento dei propri dati e gli estremi del proprio documento d'identità, il caricamento delle foto fronte e retro del proprio documento d'identità e di un video.

La verifica sulla bontà dei dati così raccolti sulla congruità del contenuto, verrà svolto in un momento successivo da personale della CA o della RA.

I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta per 20 anni dalla scadenza del certificato.

3.2.3.3 Riconoscimento effettuato secondo la modalità 3 – SPID

Nella **modalità 3 - SPID** la CA si basa su un mezzo di identificazione elettronica preesistente quale l'utilizzo di identità digitali rilasciate nel contesto del sistema SPID di livello 2 o superiore.

Il messaggio è di tipo SAML come previsto dalle specifiche CEF (Connecting Europe Facility) nell'ambito del programma CEF eID3F4, ed è inviato alla CA dal soggetto gestore del nodo nazionale ovvero da uno dei soggetti autorizzati ad avvalersi del nodo stesso. La CA verifica l'integrità del messaggio SAML ricevuto e considera identificato il soggetto sulla base dei dati contenuti nel messaggio stesso.

I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico per 20 anni dalla scadenza del certificato.

3.2.3.4 Riconoscimento effettuato secondo la modalità 4 – CIE

Nella **modalità 4 - CIE** la CA si basa su un mezzo di identificazione elettronica preesistente quale l'utilizzo della Carta d'identità elettronica (CIE) secondo le modalità previste dal portale CieID.

Il messaggio è di tipo SAML come previsto dalle specifiche CEF (Connecting Europe Facility) nell'ambito del programma CEF eID3F4, ed è inviato alla CA dal soggetto gestore del nodo nazionale ovvero da uno dei soggetti autorizzati ad avvalersi del nodo stesso. La CA verifica l'integrità del messaggio SAML ricevuto e considera identificato il soggetto sulla base dei dati contenuti nel messaggio stesso.

I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico per 20 anni dalla scadenza del certificato.

3.2.4 Identificazione della persona giuridica

n/a

3.2.5 Informazioni del Titolare o del Richiedente non verificate

n/a

3.2.6 Validazione dell'autorità

n/a

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

n/a.

3.4 Identificazione e autenticazione per le richieste di revoca

La revoca del certificato può avvenire su richiesta del Titolare o del Richiedente ovvero su iniziativa della CA.

Non è prevista la sospensione per i certificati.

3.4.1 Richiesta da parte del Titolare

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

3.4.2 Richiesta da parte del Richiedente

Il Richiedente che richiede la revoca del certificato del Soggetto si autentica sottoscrivendo l'apposito modulo di richiesta di revoca messo a disposizione dalla CA. La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 4.9.3

4 OPERATIVITÀ

4.1 Richiesta del certificato

4.1.1 Chi può richiedere un certificato

Il certificato per una persona fisica può essere richiesto da:

- Il Titolare,
 - rivolgendosi direttamente alla CA al sito www.zucchetticertifica.it, ovvero
- Il Richiedente per conto del Titolare
 - rivolgendosi direttamente alla CA mediante il sito www.zucchetticertifica.it o stipulando un accordo commerciale con la CA

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;
- 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 la responsabile del corretto funzionamento del sistema di sottoscrizione nel suo complesso, della corretta gestione dell'infrastruttura PKI e della corretta conservazione dei certificati quando non è stato diversamente concordato tra le parti.

4.2 Elaborazione della richiesta

Per ottenere un certificato di firma elettronica avanzata il Titolare e/o il Richiedente deve:

- prendere visione della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa relativa al servizio di certificazione;
- 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 che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

4.2.1 Informazioni che il Titolare deve fornire

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

- Cognome e Nome;

- Codice TIN (codice fiscale nel contesto italiano) o, in sua assenza analogo codice identificativo quale il numero del documento d'identità;
- 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.

4.2.2 Esecuzione delle funzioni di identificazione e autenticazione

Vedi §3.2

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 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.

4.3 Emissione del certificato

4.3.1 Azioni della CA durante l'emissione del certificato

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

La coppia di chiavi crittografiche viene generata sull'HSM presso la sede del TSP; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica attraverso un canale sicuro.

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, che viene memorizzato sull'HSM stesso.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

4.3.3 Attivazione

Il titolare conferma la propria identità e attiva il certificato e la firma attraverso l'inserimento di una OneTime Password ricevuta via SMS.

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

n/a

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 gli strumenti di autenticazione per la firma remota; deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo. Deve utilizzare il certificato per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.

La CA garantisce che non vengano apposte firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato il certificato e non deve apporre firme elettroniche avvalendosi di certificato emesso dalla 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 revocato controllando le relative liste nel registro dei certificati.

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 one-shot:

L'utilizzo del certificato è limitato applicativamente alla sottoscrizione dei documenti cui la firma è apposta.

The use of the certificate is technically limited to the signature of the underlying documents.

È facoltà del Soggetto o del Richiedente concordare con la 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.

Ferma restando la responsabilità della CA di cui al CAD (art.30), è responsabilità dell'Utente verificare il rispetto dei limiti d'uso inseriti nel certificato. La CA quindi non è responsabile dei danni derivanti dall'uso di un certificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

4.6 Rinnovo del certificato

4.6.1 Motivi per il rinnovo

Non è previsto il rinnovo.

4.6.2 Chi può richiedere il rinnovo

Non è previsto il rinnovo.

4.6.3 Elaborazione della richiesta di rinnovo del certificato

Non è previsto il rinnovo.

4.7 Riemissione del certificato

n/a

4.8 Modifica del certificato

n/a

4.9 Revoca del certificato

La revoca di un certificato ne toglie la validità prima della scadenza stabilita e rende non valide le firme apposte successivamente al momento della pubblicazione della revoca. I certificati revocati sono inseriti in una lista di revoca (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 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 compromesso o smarrito il dispositivo OTP;
 - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave.
2. si verifica un cambiamento dei dati del Titolare presenti nel certificato, tale da rendere detti dati non più corretti e/o veritieri;
3. termina il rapporto tra il Titolare e la CA, ovvero tra il Richiedente e la CA;
4. 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 entro la durata del certificato e per un qualunque motivo. Inoltre, la revoca del certificato può essere richiesta anche dal Richiedente, 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 tramite PEC o fax, corredata di una fotocopia di un documento di identità in corso di validità.

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

4.9.3.2 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, e se possibile la data e l'ora di decorrenza.

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.

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

I certificati revocati 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 di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata. 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.

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 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 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

n/a

4.9.14 Chi può richiedere la sospensione

n/a

4.9.15 Procedure per richiedere la sospensione

n/a

4.9.16 Limiti al periodo di sospensione

n/a

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.

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

Per l'erogazione del servizio di CA Zucchetti utilizza due Data Center: uno ubicato a Siziano (PV) e uno a Padova (PD).

Il sito di Disaster Recovery del DC di Siziano è ubicato a Roma e connesso al DC primario tramite un collegamento dedicato e ridondato su due circuiti diversi a 1Gbps caduno.

Il sito di Disaster Recovery del DC di Padova è ubicato a Milano ed è connesso al Data Center tramite un collegamento dedicato e ridondato su due circuiti diversi MPLS a 40 Gbit/s upgradabile fino a 100 Gbit/s.

All'interno di tutti i siti sopra citati 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.

Alcune componenti dei servizi di CA relativi alla pubblicazione delle CRL e all'OCSP sono ospitati su cloud AWS, rispettivamente, nella Regione Europa Milano e nella Regione Europa Irlanda.

Nell'architettura di firma elettronica avanzata, alcune componenti di orchestrazione dei servizi di Registration Authority e del Server di Firma sono ospitati su cloud AWS nella Regione Europa Milano. Per garantire inoltre la continuità operativa per la Registration Authority e il Server di firma viene eseguita una copia cifrata dei dati su cloud AWS nella Regione Europa Milano.

AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2013, 27017:2015, 27018:2019 e ISO/IEC 9001:2015.

5.1.2 Accesso fisico

L'accesso ad entrambi i Data Center è regolato da procedure di sicurezza.

Il Data Center di Siziano è certificato Tier 4.

All'interno del Data Center di Padova, certificato rating 3 secondo la ANSI TIA 942, 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

5.1.3.1 Data Center Siziano

Nel corso della progettazione del Data Center è stata tenuta in grande considerazione l'efficienza energetica tramite l'utilizzo di tecnologie avanzate per la climatizzazione.

Il campus a regime può sostenere consumi fino a 40 Mw ed è alimentato da una linea ridondata in alta tensione da 132 kV. Tutto il carico è protetto da un sistema UPS tri-ridondante in grado di assicurare il 100% di disponibilità (uptime).

Questo è reso possibile dall'architettura del sistema elettrico, ingegnerizzato secondo quanto richiesto per l'ottenimento della certificazione Tier IV Gold (modalità "system + system"(2N+1)).

Un impianto "system + system" è basato su due impianti elettrici separati, ognuno dei quali può sostenere, in ogni momento, il carico dell'intera Facility. Ogni sistema è dotato di un suo UPS (Uninterruptible Power Systems), System Bypass Modules, PDU (Power Distribution Units), RPP (Remote Power Panels) e altri componenti adeguati al livello di tiering.

Questi sistemi sono totalmente indipendenti uno dall'altro in modo da consentire tutte le attività di manutenzione, aggiornamenti e troubleshooting sia come attività pianificata che su specifica esigenza senza creare nessun impatto per l'attività dei Clienti.

Nel data center ogni sistema di alimentazione elettrica è identificato da un colore differente consentendo ai manutentori di sapere in modo univoco e ben identificabile su quale sistema di alimentazione si sta lavorando.

Tutti i rack dei clienti sono dotati di una doppia alimentazione, entrambe derivanti da due sistemi di alimentazione totalmente separati. In ogni data hall i rack sono suddivisi in isole protette da una struttura a "cage". La struttura del T-SCIF garantisce la totale compartimentazione tra l'aria calda e quella fredda, garantendo che il calore emesso dalle apparecchiature non entri in contatto con i corridoi freddi all'interno del datacenter. I rack sono installati direttamente sul pavimento, garantendo una elevata capacità di carico, che superano i limiti meccanici dei rack stessi.

Tutti i collegamenti (cablaggio strutturato, fibre ottiche, collegamenti elettrici) sono posati in apposite canaline aeree dedicate.

Il Data center offre elevati livelli di efficienza al mondo, come confermato dal parametro che misura l'efficienza energetica dei data center, pari a una media annuale P.U.E. (Power Usage Effectiveness) minore di 1,4 (valore stimato in sede di progetto).

L'impianto di raffreddamento si basa su un set modulare di AHU (Air Handling Unit) che sfruttano il principio del raffrescamento evaporativo indiretto tramite scambiatori aria-aria opportunamente raffreddati da sistemi ad acqua posti all'esterno del data center. L'infrastruttura in acciaio, che sostiene il sistema T-SCIF, ha anche la funzione di volano termico, permettendo alla Facility di raggiungere livelli di resilienza superiori ai più elevati standard di settore.

Nel DC possono essere ospitati rack ad alta densità (fino a 40KW) totalmente raffreddati ad aria.

5.1.3.2 Data Center Padova

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

5.1.4.1 Data Center Siziano

La protezione da eventuali esondazioni è garantita da un muro di cinta alto 3 mt impermeabilizzato fino ad una altezza di 1,5 mt e da una sopraelevazione rispetto l'urbanizzazione primaria di 1 mt.

È presente una vasca di laminazione atta a compensare eventuali accumuli di acqua piovana.

Il raffreddamento delle sale dati avviene tramite aria (nel DC non sono presenti tubazioni d'acqua).

Sono presenti sistemi di rilevamento anti-allagamento.

5.1.4.2 Data Center Padova

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

5.1.5.1 Data Center Siziano

Il data center ha una struttura metallica protetta da vernice intumescente e le mura perimetrali dell'area tecnica rispondono ai requisiti REI120.

Sono presenti sistemi di rilevamento anti-fumo e anti-incendio.

5.1.5.2 Data Center Padova

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

5.1.6.1 Data Center Siziano

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp (AFF-A400) e Dell EMC ISILON (F600). Per la parte SAN si è invece implementata un'infrastruttura basata su tecnologia IBM A9000.

5.1.6.2 Data Center Padova

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 per la parte data center basata su tecnologie Infinidat che comprendono n.2 enclosure InfiniBox di generazione F4000 e F6000; per la parte di CA l'infrastruttura si basa su tecnologia Pure Storage.

5.1.7 Smaltimento dei rifiuti

5.1.7.1 Data Center Siziano

Il Data Center è conforme ai requisiti della norma per il Sistema di Gestione Ambientale ISO 14001:2015. Per quel che riguarda il contenuto informativo dei rifiuti elettronici, tutti i media, prima della dismissione, vengono ripuliti secondo le procedure previste dalla procedura specifica della ISO 27001.

5.1.7.2 Data Center Padova

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

5.1.8.1 Data Center Siziano

I backup sono delocalizzati in un altro datacenter di Zucchetti, che non coincide con il sito di Disaster Recovery.

Le tecnologie utilizzate sono Rubrik per backup VM e NetApp FAS per backup con agente CommVault.

5.1.8.2 Data Center Padova

Nel sito di Disaster Recovery è presente una replica del dato ed è effettuato un backup su storage esterni terzi.

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.

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. Il coordinatore di ambito predispose il piano di formazione e lo condivide con il proprio responsabile e con l'ufficio Risorse Umane.

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.

Vengono registrati tutti gli eventi riguardanti le personalizzazioni del dispositivo di firma.
Vengono registrati tutti gli accessi fisici ai locali ad alta sicurezza dove risiedono le macchine della CA.
Vengono registrati tutti gli accessi logici alle applicazioni della CA.
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 dei documenti informatici avviene mensilmente.

5.4.3 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per 20 anni dalla CA. I log relativi al ciclo di vita del certificato rimangono in conservazione per 20 anni dalla scadenza del certificato.

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita da un sistema di conservazione dei documenti informatici.

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 dei documenti informatici.

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 anti-intrusione (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 almeno 20 anni in un sistema di conservazione dei documenti informatici.

5.5.2 Protezione dei verbali

La protezione è garantita da un Sistema di conservazione dei documenti informatici.

5.5.3 Procedure di backup dei verbali

Il sistema di conservazione dei documenti informatici 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 dei documenti informatici.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

I dati sono tutti conservati in un sistema di conservazione dei documenti informatici i quali prevedono verifiche puntuali sullo stato del sistema e l'integrità dei dati. L'esibizione dei dati avviene secondo quanto stabilito dalla norma.

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, 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.

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.

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.

Una volta accertata la compromissione della chiave privata di CA, Zucchetti procederà tempestivamente

- ad avvisare le RA e i clienti, siano essi soggetti del certificato o richiedenti, tramite comunicazione diretta, ove possibile, e tramite comunicazione sul sito Zucchetti,
- a revocare i certificati impattati, a procedere eventualmente all'emissione e accreditalmento di una nuova root CA e a fornire in maniera affidabile le informazioni sullo stato di revoca dei certificati.

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 informa della cessazione delle attività tutti i possessori di certificati da esso emessi.

In caso di cessazione della CA l'informazione sullo stato di revoca sarà fornita tramite l'emissione di un'ultima CRL conforme allo standard ETSI 319 411-1.

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 utilizzando le funzionalità native offerte dai dispositivi stessi.

6.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico che è presso il TSP Zucchetti, il quale garantisce il controllo esclusivo della chiave al titolare.

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 (root CA) è stata generata all'interno di un dispositivo crittografico sicuro. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 4096 bit oppure chiavi asimmetriche EC su una delle curve ellittiche previste dal

documento ENISA “*Agreed Cryptographic Mechanisms*” pubblicato da ENISA di lunghezza non inferiore a 256 bit.

Per le chiavi del soggetto possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bit.
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ENISA “*Agreed Cryptographic Mechanisms*” pubblicato da ENISA di lunghezza non inferiore a 256 bits.

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

6.1.7.1 Utilizzo chiave di CA

La chiave di CA viene utilizzata solamente per la firma dei certificati dei Titolari, delle Liste di Revoca e dei certificati OCSP. L'estensione KeyUsage del certificato di CA contiene firma certificati (keyCertSign) e firma CRL (cRLSign). Le risposte OCSP sono firmate tramite appositi certificati con extKeyUsage valorizzato con ocspSigning.

6.1.7.2 Utilizzo chiave del Soggetto

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.

I moduli crittografici utilizzati da Zucchetti per le chiavi di firma remota 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 di 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 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 non superiore a 16 anni, i certificati emessi a persona fisica hanno validità non superiore a 24 ore o non superiore a 72 ore per la firma remota.

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 determinazione 121/2019 [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

La descrizione dell'intero certificato è in Appendice.

7.1.3 OID dell'algoritmo di firma

I certificati sono firmati con uno dei seguenti algoritmi:

sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 11]

ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]

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

Tutte 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

Zucchetti ha richiesto una valutazione di conformità rispetto al Regolamento (Conformity Assessment Report - CAR) a un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.

Zucchetti presta il Servizio quale prestatore di servizi fiduciari 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.

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 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 rivolgendosi a commerciali e/o partner Zucchetti o scrivendo all'indirizzo signbook@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

n/a

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

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

9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili rivolgendosi a commerciali e/o partner Zucchetti o scrivendo all'indirizzo signbook@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 apposta polizza per copertura assicurativa dei rischi derivanti dall'attività descritta in questo manuale per eventuali danni causati a terzi. 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 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 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, date di revoca del certificato, non sono considerati dati personali.

9.4.4 Titolare del trattamento dei dati personali

Zucchetti S.p.A.
Piazza Mino Zucchetti, 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 risultanze 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 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 o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito; sulla segretezza e/o integrità di qualsiasi messaggio, atto o documento associato al certificato 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 rilasciati in base alle previsioni del presente Manuale e delle Condizioni del servizio.",

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. L'onere di dimostrare il dolo o la negligenza ricade sulla persona fisica o giuridica che denuncia il danno.

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, per ciascun sinistro e per anno, al canone corrisposto annualmente dal cliente.

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 Titolare.

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 regola 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.

9.12.1 Storia delle revisioni

Versione/Release n°:	1.2	Data Versione/Release:	07/01/25
Descrizione modifiche:	Cambio sede legale Inserimento algoritmi EC Inserimento certificati one shot 72 ore Aggiunta modalità di riconoscimento SPID e CIE Modifica sede DR		
Motivazioni:	Aggiornamento		

Versione/Release n°:	1.1	Data Versione/Release:	31/01/24
Descrizione modifiche:	Modifica riferimenti web e inserimento ulteriori specifiche DC		
Motivazioni:	Aggiornamento		

Versione/Release n°:	1.0	Data Versione/Release:	26/01/22
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 meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del TSP (indirizzo: www.zucchetticertifica.it);
- 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 regola 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 determinazioni successive
- [10] Determinazione AgID n°189/2017

- [11] non utilizzato
- [12] non utilizzato
- [13] Determinazione AgID n°121/2019 ver 1.1 (sostituisce deliberazione CNIPA 45/2009).

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza², nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].

9.16 Disposizioni varie

Si rimanda alla contrattualistica che regola 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 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 (*)	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.

² Disponibili sul sito <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche>

APPENDICE A - ROOT CA

Certificato di root CA Zucchetti Advanced Electronic Signature CA 2

```
0 1672: SEQUENCE {
  4 1136: SEQUENCE {
    8 3: [0] {
      10 1: INTEGER 2
      : }
      13 1: INTEGER 1
      16 13: SEQUENCE {
        18 9: OBJECT IDENTIFIER
          : sha256WithRSAEncryption (1 2 840 113549 1 1 11)
        29 0: NULL
        : }
      31 156: 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 31: SET {
              76 29: SEQUENCE {
                78 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
                83 22: UTF8String 'Trust Service Provider'
                : }
                : }
            107 26: SET {
              109 24: SEQUENCE {
                111 3: OBJECT IDENTIFIER '2 5 4 97'
                116 17: UTF8String 'VATIT-05006900962'
                : }
                : }
            135 53: SET {
              137 51: SEQUENCE {
                139 3: OBJECT IDENTIFIER commonName (2 5 4 3)
                144 44: UTF8String
                  : 'Zucchetti Advanced Electronic Signature CA 2'
                  : }
                  : }
                  : }
```

Certificati di Sottoscrizione Manuale Operativo ZUCCHETTI-MO-FEA

```
190 30: SEQUENCE {
192 13:  UTCTime 14/12/2021 10:32:01 GMT
207 13:  UTCTime 14/12/2037 11:32:01 GMT
      :  }
222 156: SEQUENCE {
225 11:  SET {
227 9:   SEQUENCE {
229 3:   OBJECT IDENTIFIER countryName (2 5 4 6)
234 2:   PrintableString 'IT'
      :   }
      :   }
238 25:  SET {
240 23:  SEQUENCE {
242 3:   OBJECT IDENTIFIER organizationName (2 5 4 10)
247 16:  UTF8String 'Zucchetti S.p.A.'
      :   }
      :   }
265 31:  SET {
267 29:  SEQUENCE {
269 3:   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
274 22:  UTF8String 'Trust Service Provider'
      :   }
      :   }
298 26:  SET {
300 24:  SEQUENCE {
302 3:   OBJECT IDENTIFIER '2 5 4 97'
307 17:  UTF8String 'VATIT-05006900962'
      :   }
      :   }
326 53:  SET {
328 51:  SEQUENCE {
330 3:   OBJECT IDENTIFIER commonName (2 5 4 3)
335 44:  UTF8String
      :   'Zucchetti Advanced Electronic Signature CA 2'
      :   }
      :   }
      :   }
381 546: SEQUENCE {
385 13:  SEQUENCE {
387 9:   OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
398 0:   NULL
      :   }
400 527: BIT STRING, encapsulates {
405 522: SEQUENCE {
409 513: INTEGER
      :   00 C8 70 4A E2 1C 83 9B D9 32 61 C3 EB 4A 73 88
      :   57 44 DA B6 70 58 8B 5D DD 03 29 B2 84 56 F1 D6
      :   16 CC FC 37 21 D7 44 2D F1 E6 63 23 9A 84 A2 60
```

Certificati di Sottoscrizione Manuale Operativo ZUCCHETTI-MO-FEA

```
      : DE D2 B8 98 11 24 20 79 39 70 2D D2 3D 68 B0 7F
      : B1 55 12 8A 38 E8 88 AA 0E FE C0 CD DC 74 29 13
      : 1F 78 4C DD F5 CF 6E D0 8C 66 28 86 7C 96 25 C1
      : ED 99 67 1B 9C 93 BA 7E 44 B0 F4 F3 42 4B A7 88
      : EE DA 9F 1B 18 D0 6F EA 62 E0 BC 0E AF 4D E2 52
      : [ Another 385 bytes skipped ]
926 3: INTEGER 65537
      : }
      : }
      : }
931 210: [3] {
934 207: SEQUENCE {
937 15: SEQUENCE {
939 3: OBJECT IDENTIFIER basicConstraints (2 5 29 19)
944 1: BOOLEAN TRUE
947 5: OCTET STRING, encapsulates {
949 3: SEQUENCE {
951 1: BOOLEAN TRUE
      : }
      : }
      : }
954 73: SEQUENCE {
956 3: OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
961 66: OCTET STRING, encapsulates {
963 64: SEQUENCE {
965 62: SEQUENCE {
967 4: OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
973 54: SEQUENCE {
975 52: SEQUENCE {
977 8: OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
987 40: IA5String 'https://ca.zucchetticertifica.it/doc/mo/'
      : }
      : }
      : }
      : }
      : }
1029 66: SEQUENCE {
1031 3: OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1036 59: OCTET STRING, encapsulates {
1038 57: SEQUENCE {
1040 55: SEQUENCE {
1042 53: [0] {
1044 51: [0] {
1046 49: [6]
      : 'http://crl.ca2.zucchetticertifica.it/ades/ARL.cr'
      : '|'
      : }
```

```

:      }
:      }
:      }
:      }
:      }
1097 14: SEQUENCE {
1099 3:  OBJECT IDENTIFIER keyUsage (2 5 29 15)
1104 1:  BOOLEAN TRUE
1107 4:  OCTET STRING, encapsulates {
1109 2:  BIT STRING 1 unused bit
:      '1100000'B
:      }
:      }
1113 29: SEQUENCE {
1115 3:  OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1120 22: OCTET STRING, encapsulates {
1122 20: OCTET STRING
:      09 B4 D9 CC F2 AC 9E ED 6F B2 13 B5 5F EB 56 3B
:      DC 55 D7 54
:      }
:      }
:      }
:      }
:      }
1144 13: SEQUENCE {
1146 9:  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1157 0:  NULL
:      }
1159 513: BIT STRING
:      81 B1 93 1E E8 99 4D E7 83 B2 9B A9 00 B8 EF 04
:      80 B4 25 0B D4 F8 E2 5F 84 D0 1A 94 C1 E1 23 61
:      39 C8 9E A8 11 C9 AB D5 E0 00 54 35 EC E1 1F B0
:      DF 01 A5 D3 E4 66 E9 93 D2 7B D9 9F 34 DC 24 D6
:      EA CD 57 85 7E D8 CA 77 8A 6E C1 DA 5D 2B 0E BD
:      97 D7 C3 91 8E 8B 60 4E 24 B9 EF 9C CD A0 F5 7B
:      4B 96 BB C4 3E E1 2E 15 9F 1E 08 D2 80 9E CB 71
:      76 B0 44 66 47 66 DF C4 BF 1F F5 02 D9 F9 75 D4
:      [ Another 384 bytes skipped ]
:      }
```

Certificato di root CA Zucchetti Advanced Electronic Signature EC CA 2

```
0 853: SEQUENCE {
  4 730: SEQUENCE {
    8 3: [0] {
      10 1: INTEGER 2
      : }
    13 20: INTEGER 12 91 2C B2 C3 B5 28 38 F9 13 B1 1B A0 EE 42 97 61 82 F8 6E
    35 10: SEQUENCE {
      37 8: OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
      : }
    47 159: SEQUENCE {
      50 11: SET {
        52 9: SEQUENCE {
          54 3: OBJECT IDENTIFIER countryName (2 5 4 6)
          59 2: PrintableString 'IT'
          : }
        : }
      63 25: SET {
        65 23: SEQUENCE {
          67 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
          72 16: UTF8String 'Zucchetti S.p.A.'
          : }
        : }
      90 31: SET {
        92 29: SEQUENCE {
          94 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
          99 22: UTF8String 'Trust Service Provider'
          : }
        : }
      123 26: SET {
        125 24: SEQUENCE {
          127 3: OBJECT IDENTIFIER '2 5 4 97'
          132 17: UTF8String 'VATIT-05006900962'
          : }
        : }
      151 56: SET {
        153 54: SEQUENCE {
          155 3: OBJECT IDENTIFIER commonName (2 5 4 3)
          160 47: UTF8String
            : 'Zucchetti Advanced Electronic Signature EC CA 2'
            : }
        : }
      : }
    209 30: SEQUENCE {
      211 13: UTCTime 20/05/2024 09:20:51 GMT
      226 13: UTCTime 20/05/2037 09:20:51 GMT
      : }
  }
```

```
241 159: SEQUENCE {
244 11:   SET {
246 9:    SEQUENCE {
248 3:     OBJECT IDENTIFIER countryName (2 5 4 6)
253 2:     PrintableString 'IT'
      :   }
      : }
257 25: SET {
259 23:  SEQUENCE {
261 3:   OBJECT IDENTIFIER organizationName (2 5 4 10)
266 16:  UTF8String 'Zucchetti S.p.A.'
      :  }
      : }
284 31: SET {
286 29:  SEQUENCE {
288 3:   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
293 22:  UTF8String 'Trust Service Provider'
      :  }
      : }
317 26: SET {
319 24:  SEQUENCE {
321 3:   OBJECT IDENTIFIER '2 5 4 97'
326 17:  UTF8String 'VATIT-05006900962'
      :  }
      : }
345 56: SET {
347 54:  SEQUENCE {
349 3:   OBJECT IDENTIFIER commonName (2 5 4 3)
354 47:  UTF8String
      :   'Zucchetti Advanced Electronic Signature EC CA 2'
      :   }
      : }
403 118: SEQUENCE {
405 16:  SEQUENCE {
407 7:   OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
416 5:   OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
      :   }
423 98:  BIT STRING
      :   04 75 59 EF 8F CB 26 27 19 8E 98 6C 53 05 96 DF
      :   A3 B3 ED 94 02 8F 25 B9 BD 22 1C D1 94 96 4D ED
      :   62 D4 EF 2C 42 59 81 21 3B B4 F1 D8 28 7C 79 95
      :   16 3D D3 D9 0A E0 CA 4B 2A B7 DA EA 0C 99 35 52
      :   3B 1F B6 84 83 E3 FC 88 55 BC 42 75 59 0C A2 9B
      :   C3 71 D9 2E 6A AC 75 05 0C 0D 5D 04 F2 71 7E FD
      :   2B
      : }
523 212: [3] {
526 209: SEQUENCE {
```

```

529 15: SEQUENCE {
531 3:  OBJECT IDENTIFIER basicConstraints (2 5 29 19)
536 1:  BOOLEAN TRUE
539 5:  OCTET STRING, encapsulates {
541 3:    SEQUENCE {
543 1:      BOOLEAN TRUE
      :    }
      :  }
      : }
546 73: SEQUENCE {
548 3:  OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
553 66: OCTET STRING, encapsulates {
555 64:   SEQUENCE {
557 62:     SEQUENCE {
559 4:       OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
565 54:       SEQUENCE {
567 52:         SEQUENCE {
569 8:           OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
579 40:           IA5String 'https://ca.zucchetticertifica.it/doc/mo/'
           :         }
           :       }
           :     }
           :   }
           : }
621 68: SEQUENCE {
623 3:  OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
628 61: OCTET STRING, encapsulates {
630 59:   SEQUENCE {
632 57:     SEQUENCE {
634 55:       [0] {
636 53:         [0] {
638 51:           [6]
           :         'http://crl.ca2.zucchetticertifica.it/adesecc/ARL.'
           :         'crl'
           :       }
           :     }
           :   }
           : }
           : }
691 14: SEQUENCE {
693 3:  OBJECT IDENTIFIER keyUsage (2 5 29 15)
698 1:  BOOLEAN TRUE
701 4:  OCTET STRING, encapsulates {
703 2:    BIT STRING 1 unused bit
      :    '1100000'B
      :  }
      : }

```

```
707 29: SEQUENCE {
709 3: OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
714 22: OCTET STRING, encapsulates {
716 20: OCTET STRING
: CC 8C 04 6A F0 96 53 8C BF 7E 45 7D 51 5C C3 F3
: E5 2E 7C 3E
: }
: }
: }
: }
: }
: }
738 10: SEQUENCE {
740 8: OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
: }
750 105: BIT STRING, encapsulates {
753 102: SEQUENCE {
755 49: INTEGER
: 00 E9 AB D2 70 6D F6 0F DA D9 36 D7 8D 7A B5 5D
: 0E 41 34 09 40 3A D8 69 96 F0 27 B5 3E AE 6E 41
: 1E E3 8F 20 41 D9 1D 44 FF 5C 76 18 44 45 F2 EC
: E1
806 49: INTEGER
: 00 E7 7A 5D 0B E3 3E 2F FA D4 BF E4 CB FA 69 3F
: C7 85 6D 65 19 66 52 19 19 D5 00 0B 5A 28 12 BF
: 2B 65 1A 40 1D 17 B7 27 39 25 AD 2F 74 C2 0B 51
: 6B
: }
: }
: }
```

Certificato titolare Zucchetti Advanced Electronic Signature CA 2

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:	Trust Service Provider
Organization Identifier:	VATIT-05006900962
Common Name:	Zucchetti Advanced Electronic Signature CA 2
VALIDITY:	24 hours/72 hours
Not Before:	
Not After:	
SUBJECT:	
Country Name:	<i>CountryCode (ISO 3166) (mandatory)</i>
Organization Name:	<i>(conditioned presence) (*)</i>
Organizational Unit Name:	<i>(conditioned presence) (*)</i>
Organization Identifier:	<i>(conditioned presence) (*)</i>
GivenName:	<i>Name</i>
Surname:	<i>Surname</i>
SerialNumber:	<i>(mandatory)</i>
Title:	<i>Holder's specific qualification (optional)</i>
Locality:	<i>(optional) (**)</i>
DNQualifier:	<i>Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)</i>
Common Name:	<i>name of the subject (recommended)</i>
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.ca2.zuccheticertifica.it/ades/CRL\$\$\$.crl	

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

Authority Information Access	
Access Method	
Alternative Name	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.ad.es.ca2.zucchetticertifica.it
Subject Key Identifier:	1.3.6.1.5.5.7.48.2
SubjectDirectoryAttributes	http://crl.ca2.zucchetticertifica.it/ades/CA.crt
DateOfBirth	key identifier (sha1 (160 bit) of public key)
Subject Alternative Name	
RFC822Name	
Certificate Policies:	
Policy 1:	<i>certificate holder e-mail</i>
Policy ID:	
Policy 2:	
Policy ID:	<ul style="list-style-type: none"> • 0.4.0.2042.1.2
Policy 3:	
Policy ID:	<ul style="list-style-type: none"> • 1.3.76.45.1.1.8 (24h) • 1.3.76.45.1.1.9 (72h)
Policy Qualifier ID:	
CPS url:	https://ca.zucchetticertifica.it/doc/mo/
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
<p><i>(*)</i>: when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as <i>organizationName</i> and <i>organizationIdentifier</i></p> <p><i>(**)</i>: if the organization attribute is present, it contains information relevant to the specified organization.</p> <p>NB: xx = <i>partitioned revocation list progressive numbering</i></p>	

Certificato titolare Zucchetti Advanced Electronic Signature CA 2

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:	Trust Service Provider
Organization Identifier:	VATIT-05006900962
Common Name:	Zucchetti Advanced Electronic Signature EC CA 2
VALIDITY:	24 hours
Not Before:	
Not After:	
SUBJECT:	
Country Name:	<i>CountryCode (ISO 3166) (mandatory)</i>
Organization Name:	<i>(conditioned presence) (*)</i>
Organizational Unit Name:	<i>(conditioned presence) (*)</i>
Organization Identifier:	<i>(conditioned presence) (*)</i>
GivenName:	<i>Name</i>
Surname:	<i>Surname</i>
SerialNumber:	<i>(mandatory)</i>
Title:	<i>Holder's specific qualification (optional)</i>
Locality:	<i>(optional) (**)</i>
DNQualifier:	<i>Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)</i>
Common Name:	<i>name of the subject (recommended)</i>
PUBLIC KEY:	EC asymmetric keys on one of the elliptic curves provided for by the ENISA "Agreed Cryptographic Mechanisms" with a length of no less than 384 bits
ALGORITHM:	
ALG. ID:	-
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	

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

ID1:	
	http://crl.ca2.zucchetticertifica.it/adeseccrl\$.crl
Authority Information Access	
Access Method	
Alternative Name	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.adeseccrl.ca2.zucchetticertifica.it
Subject Key Identifier:	1.3.6.1.5.5.7.48.2
SubjectDirectoryAttributes	http://crl.ca2.zucchetticertifica.it/adeseccrl\$.crl
DateOfBirth	key identifier (sha1 (160 bit) of public key)
Subject Alternative Name RFC822Name	
Certificate Policies:	
Policy 1:	<i>certificate holder e-mail</i>
Policy ID:	
Policy 2:	
Policy ID:	<ul style="list-style-type: none"> • 0.4.0.2042.1.2
Policy 3:	
Policy ID:	<ul style="list-style-type: none"> • 1.3.76.45.1.1.11
Policy Qualifier ID:	
CPS url:	https://ca.zucchetticertifica.it/doc/mo/
SIGNATURE:	
ALG. ID:	–
PARAMETER:	0
VALUE:	Ca Signature
<p>(*): 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</p> <p>(**): if the organization attribute is present, it contains information relevant to the specified organization.</p> <p>NB: xx = partitioned revocation list progressive numbering</p>	

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 Advanced Electronic Signature CA 2 organizationIdentifier=VATIT-05006900962 OU=Trust Service Provider 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
Issuer's Signature	Firma della CA

Estensione	Valore
Issuer Signature Algorithm	ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]
Issuer Distinguished Name	CN=Zucchetti Advanced Electronic Signature EC CA 2 organizationIdentifier=VATIT-05006900962 OU=Trust Service Provider 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
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 (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:

Certificati di Sottoscrizione
Manuale Operativo ZUCCHETTI-MO-FEA

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
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] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
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	sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(1 13549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] OR ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] OR ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)] OR ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
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 requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in una responseExtensions.