

# Manuale Operativo

## Certificate Practice Statement

CODICE DOCUMENTO	ICERT-INDI-FEA
VERSIONE	1.7
DATA	15/05/2024

# SOMMARIO

<b>1</b>	<b>INTRODUZIONE .....</b>	<b>7</b>
1.1	Quadro generale .....	7
1.2	Nome ed identificativo del documento .....	7
1.3	Partecipanti e responsabilità .....	8
1.3.1	Certification Authority – Autorità di Certificazione .....	8
1.3.2	Registration authority – Ufficio di Registrazione (RA) .....	9
1.3.3	Soggetto .....	10
1.3.4	Utente .....	10
1.3.5	Richiedente .....	10
1.3.6	Autorità .....	11
1.4	Uso del certificato .....	11
1.4.1	Usi consentiti .....	11
1.4.2	Usi non consentiti .....	11
1.5	Amministrazione del Manuale Operativo .....	11
1.5.1	Amministratore del Manuale Operativo .....	11
1.5.2	Contatti .....	11
1.5.3	Soggetti responsabili dell'approvazione del Manuale Operativo .....	12
1.5.4	Procedure di approvazione .....	12
1.6	Definizioni e acronimi .....	12
1.6.1	Definizioni .....	12
1.6.2	Acronimi e abbreviazioni: .....	18
<b>2</b>	<b>PUBBLICAZIONE E ARCHIVIAZIONE .....</b>	<b>21</b>
2.1	Archiviazione .....	21
2.2	Pubblicazione delle informazioni sulla certificazione .....	21
2.2.1	Pubblicazione del manuale operativo .....	21
2.2.2	Pubblicazione dei certificati .....	21
2.2.3	Pubblicazione delle liste di revoca e sospensione .....	21
2.3	Periodo o frequenza di pubblicazione .....	21
2.3.1	Frequenza di pubblicazione del manuale operativo .....	21
2.3.2	Frequenza pubblicazione delle liste di revoca e sospensione .....	21
2.4	Controllo degli accessi agli archivi pubblici .....	21
<b>3</b>	<b>IDENTIFICAZIONE E AUTENTICAZIONE .....</b>	<b>23</b>
3.1	Denominazione .....	23
3.1.1	Tipi di nomi .....	23
3.1.2	Necessità che il nome abbia un significato .....	23
3.1.3	Anonimato e pseudonimia dei richiedenti .....	23
3.1.4	Regole di interpretazione dei tipi di nomi .....	23
3.1.5	Univocità dei nomi .....	23
3.1.6	Riconoscimento, autenticazione e ruolo dei marchi registrati .....	24
3.2	Convalida iniziale dell'identità .....	24
3.2.1	Metodo per dimostrare il possesso della chiave privata .....	24
3.2.2	Autenticazione dell'identità delle organizzazioni .....	24
3.2.3	Identificazione della persona fisica .....	24
3.2.4	Identificazione della persona giuridica .....	30
3.2.5	Informazioni del Soggetto o del Richiedente non verificate .....	30
3.2.6	Validazione dell'autorità .....	30
3.3	Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati .....	30
3.3.1	Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati .....	30
3.4	Identificazione e autenticazione per le richieste di revoca o sospensione .....	30
3.4.1	Richiesta da parte del Soggetto .....	31
3.4.2	Richiesta da parte del Richiedente .....	31

<b>4</b>	<b>OPERATIVITÀ</b>	<b>32</b>
4.1	Richiesta del certificato	32
4.1.1	Chi può richiedere un certificato	32
4.1.2	Processo di registrazione e responsabilità	32
4.2	Elaborazione della richiesta	33
4.2.1	Informazioni che il Soggetto deve fornire	33
4.2.2	Esecuzione delle funzioni di identificazione e autenticazione	34
4.2.3	Approvazione o rifiuto della richiesta del certificato	35
4.2.4	Tempo massimo per l'elaborazione della richiesta del certificato	35
4.3	Emissione del certificato	35
4.3.1	Azioni della CA durante l'emissione del certificato	35
4.3.2	Notifica ai richiedenti dell'avvenuta emissione del certificato	36
4.3.3	Attivazione	37
4.4	Accettazione del certificato	37
4.4.1	Comportamenti concludenti di accettazione del certificato	37
4.4.2	Pubblicazione del certificato da parte della Certification Authority	37
4.4.3	Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato	37
4.5	Uso della coppia di chiavi e del certificato	37
4.5.1	Uso della chiave privata e del certificato da parte del Soggetto	37
4.5.2	Uso della chiave pubblica e del certificato da parte degli Utenti Finali	38
4.5.3	Limiti d'uso e di valore	38
4.6	Rinnovo del certificato	38
4.6.1	Motivi per il rinnovo	38
4.6.2	Chi può richiedere il rinnovo	38
4.6.3	Elaborazione della richiesta di rinnovo del certificato	39
4.7	Rimissione del certificato	39
4.8	Modifica del certificato	39
4.9	Revoca e sospensione del certificato	39
4.9.1	Motivi per la revoca	39
4.9.2	Chi può richiedere la revoca	40
4.9.3	Procedure per richiedere la revoca	40
4.9.4	Periodo di grazia della richiesta di revoca	41
4.9.5	Tempo massimo di elaborazione della richiesta di revoca	41
4.9.6	Requisiti per la verifica della revoca	41
4.9.7	Frequenza di pubblicazione della CRL	41
4.9.8	Latenza massima della CRL	42
4.9.9	Servizi online di verifica dello stato di revoca del certificato	42
4.9.10	Requisiti servizi on line di verifica	42
4.9.11	Altre forme di revoca	42
4.9.12	Requisiti specifici rekey in caso di compromissione	42
4.9.13	Motivi per la sospensione	42
4.9.14	Chi può richiedere la sospensione	43
4.9.15	Procedure per richiedere la sospensione	43
4.9.16	Limiti al periodo di sospensione	44
4.10	Servizi riguardanti lo stato del certificato	44
4.10.1	Caratteristiche operative	44
4.10.2	Disponibilità del servizio	45
4.10.3	Caratteristiche opzionali	45
4.11	Disdetta dai servizi della CA	45
4.12	Deposito presso terzi e recovery della chiave	45
<b>5</b>	<b>MISURE DI SICUREZZA E CONTROLLI</b>	<b>46</b>
5.1	Sicurezza fisica	46
5.1.1	Posizione e costruzione della struttura	46
5.1.2	Accesso fisico	47
5.1.3	Impianto elettrico e di climatizzazione	48
5.1.4	Prevenzione e protezione contro gli allagamenti	48

5.1.5	Prevenzione e protezione contro gli incendi .....	49
5.1.6	Supporti di memorizzazione .....	49
5.1.7	Smaltimento dei rifiuti .....	49
5.1.8	Off-site backup .....	49
5.2	Controlli procedurali .....	50
5.2.1	Ruoli chiave .....	50
5.3	Controllo del personale .....	50
5.3.1	Qualifiche, esperienze e autorizzazioni richieste .....	50
5.3.2	Procedure di controllo delle esperienze pregresse .....	50
5.3.3	Requisiti di formazione .....	50
5.3.4	Frequenza di aggiornamento della formazione .....	51
5.3.5	Frequenza nella rotazione dei turni di lavoro .....	51
5.3.6	Sanzioni per azioni non autorizzate .....	51
5.3.7	Controlli sul personale non dipendente .....	51
5.3.8	Documentazione che il personale deve fornire .....	51
5.4	Gestione del giornale di controllo .....	52
5.4.1	Tipi di eventi memorizzati .....	52
5.4.2	Frequenza di trattamento e di memorizzazione del giornale di controllo .....	52
5.4.3	Periodo di conservazione del giornale di controllo .....	52
5.4.4	Protezione del giornale di controllo .....	52
5.4.5	Procedure di backup del giornale di controllo .....	52
5.4.6	Sistema di memorizzazione del giornale di controllo .....	53
5.4.7	Notifica in caso di identificazione di vulnerabilità .....	53
5.4.8	Valutazioni di vulnerabilità .....	53
5.5	Archiviazione dei verbali .....	53
5.5.1	Tipi di verbali archiviati .....	53
5.5.2	Protezione dei verbali .....	53
5.5.3	Procedure di backup dei verbali .....	53
5.5.4	Requisiti per la marcatura temporale dei verbali .....	53
5.5.5	Sistema di memorizzazione degli archivi .....	53
5.5.6	Procedure per ottenere e verificare le informazioni contenute negli archivi .....	53
5.6	Sostituzione della chiave privata della CA .....	54
5.7	Compromissione della chiave privata della CA e disaster recovery .....	54
5.7.1	Procedure per la gestione degli incidenti .....	54
5.7.2	Corruzione delle macchine, del software o dei dati .....	54
5.7.3	Procedure in caso di compromissione della chiave privata della CA .....	54
5.7.4	Erogazione dei servizi di CA in caso di disastri .....	55
5.8	Cessazione del servizio della CA o della RA .....	55
<b>6</b>	<b>CONTROLLI DI SICUREZZA TECNOLOGICA .....</b>	<b>56</b>
6.1	Installazione e generazione della coppia di chiavi di certificazione .....	56
6.1.1	Generazione della coppia di chiavi del Soggetto .....	56
6.1.2	Consegna della chiave privata al Richiedente .....	57
6.1.3	Consegna della chiave pubblica alla CA .....	57
6.1.4	Consegna della chiave pubblica agli utenti .....	57
6.1.5	Algoritmo e lunghezza delle chiavi .....	57
6.1.6	Controlli di qualità e generazione della chiave pubblica .....	57
6.1.7	Scopo di utilizzo della chiave .....	58
6.2	Protezione della chiave privata e controlli ingegneristici del modulo crittografico .....	58
6.2.1	Controlli e standard del modulo crittografico .....	58
6.2.2	Controllo di più persone della chiave privata di CA .....	58
6.2.3	Deposito presso terzi della chiave privata di CA .....	58
6.2.4	Backup della chiave privata di CA .....	58
6.2.5	Archiviazione della chiave privata di CA .....	59
6.2.6	Trasferimento della chiave privata da un modulo o su un modulo crittografico .....	59
6.2.7	Memorizzazione della chiave privata su modulo crittografico .....	59
6.2.8	Metodo di attivazione della chiave privata .....	59

6.2.9	Metodo di disattivazione della chiave privata .....	59
6.2.10	Metodo per distruggere la chiave privata della CA .....	59
6.2.11	Classificazione dei moduli crittografici .....	59
6.3	Altri aspetti della gestione delle chiavi .....	59
6.3.1	Archiviazione della chiave pubblica .....	60
6.3.2	Periodo di validità del certificato e della coppia di chiavi .....	60
6.4	Dati di attivazione della chiave privata .....	60
6.5	Controlli sulla sicurezza informatica .....	60
6.5.1	Requisiti di sicurezza specifici dei computer .....	60
6.6	Operatività sui sistemi di controllo .....	60
6.7	Controlli di sicurezza della rete .....	61
6.1	Controlli di sicurezza della rete .....	61
<b>7</b>	<b>FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP .....</b>	<b>63</b>
7.1	Formato del certificato .....	63
7.1.1	Numero di versione .....	63
7.1.2	Estensioni del certificato .....	63
7.1.3	OID dell'algoritmo di firma .....	63
7.1.4	Forme di nomi .....	64
7.1.5	Vincoli ai nomi .....	64
7.1.6	OID del certificato .....	64
7.2	Formato della CRL .....	64
7.2.1	Numero di versione .....	64
7.2.2	Estensioni della CRL .....	64
7.3	Formato dell'OCSP .....	64
7.3.1	Numero di versione .....	64
7.3.2	Estensioni dell'OCSP .....	64
<b>8</b>	<b>CONTROLLI E VALUTAZIONI DI CONFORMITÀ .....</b>	<b>65</b>
8.1	Frequenza o circostanze per la valutazione di conformità .....	65
8.2	Identità e qualifiche di chi effettua il controllo .....	65
8.3	Rapporti tra InfoCert e CAB .....	65
8.4	Aspetti oggetto di valutazione .....	66
8.5	Azioni in caso di non conformità .....	66
<b>9</b>	<b>ALTRI ASPETTI LEGALI E DI BUSINESS .....</b>	<b>67</b>
9.1	Tariffe .....	67
9.1.1	Tariffe per il rilascio e il rinnovo dei certificati .....	67
9.1.2	Tariffe per l'accesso ai certificati .....	67
9.1.3	Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati .....	67
9.1.4	Tariffe per altri servizi .....	67
9.1.5	Politiche per il rimborso .....	67
9.2	Responsabilità finanziaria .....	67
9.2.1	Copertura assicurativa .....	67
9.2.2	Altre attività .....	68
9.2.3	Garanzia o copertura assicurativa per i soggetti finali .....	68
9.3	Confidenzialità delle informazioni di business .....	68
9.3.1	Ambito di applicazione delle informazioni confidenziali .....	68
9.3.2	Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali .....	68
9.3.3	Responsabilità di protezione delle informazioni confidenziali .....	68
9.4	Privacy .....	68
9.4.1	Programma sulla privacy .....	68
9.4.2	Dati che sono trattati come personali .....	69
9.4.3	Dati non considerati come personali .....	69
9.4.4	Titolare del trattamento .....	69
9.4.5	Informativa privacy e consenso al trattamento dei dati personali .....	69
9.4.6	Divulgazione dei dati a seguito di richiesta da parte dell'Autorità .....	69
9.4.7	Altri motivi di divulgazione .....	69

9.5	Proprietà intellettuale .....	70
9.6	Rappresentanza e garanzie.....	70
9.7	Limitazione di garanzia .....	70
9.8	Limitazione di responsabilità.....	70
9.9	Indennizzi.....	70
9.10	Termine e risoluzione .....	70
9.10.1	Termine.....	70
9.10.2	Risoluzione .....	70
9.10.3	Effetti della risoluzione.....	70
9.11	Canali di comunicazione ufficiali.....	70
9.12	Revisione del Manuale Operativo.....	71
9.12.1	Storia delle revisioni.....	71
9.12.2	Procedure di revisione .....	75
9.12.3	Periodo e meccanismo di notifica .....	75
9.12.4	Casi nei quali l’OID deve cambiare.....	75
9.13	Risoluzione delle controversie .....	75
9.14	Foro competente.....	76
9.15	Legge applicabile.....	76
9.16	Disposizioni varie .....	77
9.17	Altre disposizioni .....	77
<b>APPENDICE A .....</b>		<b>78</b>
	Certificato di ROOT: InfoCert Advanced Electronic Signature CA 3.....	78
	Certificato di ROOT: InfoCert Advanced Electronic Signature CA 4.....	84
	Certificato di ROOT: InfoCert Advanced Electronic Signature EC CA 4 .....	92
	Formato delle CRL e OCSP .....	98
	Valori ed estensioni per CRL e OCSP .....	99
	OCSP Extensions.....	101

## INDICE DELLE FIGURE

<b>Figura 1 - ubicazione Data Center InfoCert e sito della Disaster Recovery .....</b>	<b>47</b>
--	-----------

# 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 o giuridica è il **Soggetto** 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 Soggetto. Il grado d'affidabilità di quest'associazione è legato a diversi fattori: la modalità con cui la Certification Authority (di seguito, anche semplicemente, "CA") 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 InfoCert S.p.A.** (*Trust Service Provider*) (nel prosieguo, anche semplicemente, "InfoCert") che, tra i servizi fiduciari, fornisce anche servizi di firma elettronica avanzata e sigillo elettronico avanzato. 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, firma elettronica avanzata ovvero sigillo elettronico avanzato.

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 Soggetto.

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 ed identificativo del documento

Questo documento è denominato "Prestatore di Servizi Fiduciari InfoCert – Manuale Operativo" ed è caratterizzato dal codice documento: **ICERT-INDI-FEA**. La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

Al documento sono associati gli Object Identifier (OID), descritti in 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 InfoCert è 1.3.76.36

DESCRIZIONE	OID
<b>Manuale-operativo-certificato emesso a persona fisica</b>	1.3.76.36.1.1.8.1 conforme alla policy NCP. 0.4.0.2042.1.1
<b>Manuale-operativo-certificato emesso a persona fisica e chiavi su dispositivo (SSCD)</b>	1.3.76.36.1.1.8.3 conforme alla policy NCP+ 0.4.0.2042.1.2
<b>Manuale-operativo-certificato emesso a persona fisica per firma automatica remota su dispositivo</b>	1.3.76.36.1.1.8.5 conforme alla policy NCP+ 0.4.0.2042.1.2
<b>Manuale-operativo-certificato emesso a persona giuridica</b>	1.3.76.36.1.1.8.2 conforme alla policy NCP 0.4.0.2042.1.1
<b>Manuale-operativo-certificato emesso a persona giuridica e chiavi su dispositivo (SSCD)</b>	1.3.76.36.1.1.8.4 conforme alla policy NCP+ 0.4.0.2042.1.2
<b>Manuale-operativo-certificato emesso a persona giuridica per firma automatica remota su dispositivo</b>	1.3.76.36.1.1.8.6 conforme alla policy NCP+ 0.4.0.2042.1.2
<b>Manuale-operativo-certificato emesso a solo scopo di test</b>	1.3.76.36.1.1.8.9 conforme alla policy NCP+ 0.4.0.2042.1.2

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 Prestatore di Servizi Fiduciari all'indirizzo: <https://www.firma.infocert.it> ovvero <https://www.infocert.it>, sezione "Documentazione".

## 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.

InfoCert 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 [2].

I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

<b>Denominazione sociale</b>	InfoCert – Società per azioni Società soggetta a direzione e coordinamento di Tinexta S.p.A.
<b>Sede legale</b>	Piazza Sallustio n.9, 00187, Roma (RM)
<b>Sedi operative</b>	Via Marco e Marcelliano n.45, 00147, Roma (RM) Via Fernanda Wittgens n. 2, 20123 Milano (MI) Piazza Luigi da Porto n. 3, 35131 Padova (PD)
<b>Rappresentante legale</b>	Danilo Cattaneo In qualità di Amministratore Delegato
<b>N. di telefono</b>	06 836691
<b>Codice fiscale e n. Iscrizione Registro Imprese</b>	07945211006
<b>Numero REA</b>	RM - 1064345
<b>N. partita IVA</b>	07945211006
<b>Sito web</b>	<a href="https://www.infocert.it">https://www.infocert.it</a>

### 1.3.2 Registration authority – Ufficio di Registrazione (RA)

Le **Registration Authorities o Uffici di Registrazione** (di seguito, anche semplicemente, **"RA"**) 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 Soggetto o del Richiedente,
- la registrazione dei dati del Soggetto,
- l'inoltro dei dati del Soggetto ai sistemi della CA,

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

La Registration Authority svolge, in sostanza tutte le attività di interfaccia tra la Certification Authority e il Soggetto o il Richiedente, in base agli accordi intercorsi.

#### **1.3.2.1 Incaricato alla Registrazione (IR) o Registration Authority Officer**

La RA può nominare persone fisiche o giuridiche cui affidare lo svolgimento delle attività di identificazione del Soggetto. Gli **Incaricati alla Registrazione** o Registration Authority Officer operano sulla base delle istruzioni ricevute dalla RA, cui fanno riferimento e che ha compiti di vigilanza sulla correttezza delle procedure attuate. Nel prosieguo del documento, tali soggetti verranno qualificati unicamente come Incaricati alla Registrazione.

#### **1.3.3 Soggetto**

E' la persona fisica o giuridica 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 digitale del Soggetto, e che fa affidamento sulla validità del certificato medesimo (e/o sulla firma avanzata ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

#### **1.3.5 Richiedente**

È la persona fisica o giuridica che richiede alla CA il rilascio di certificati digitali per un Soggetto, eventualmente sostenendone i costi e assumendo la facoltà di sospendere o revocare i certificati stessi. Il ruolo, quando presente, può essere assunto anche dalla RA.

Nello specifico si individuano le seguenti casistiche:

- può coincidere con il Soggetto se questi è una persona fisica,
- può essere la persona fisica che ha i poteri di richiedere un certificato per una persona giuridica,
- 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 Soggetto.

## **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 di certificazione, qualificati e non, 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 alle normative e agli standard applicabili, del prestatore di servizi fiduciari qualificato per i servizi qualificati e non qualificati da esso prestati.

## **1.4 Uso del certificato**

### **1.4.1 Usi consentiti**

I certificati emessi dalla CA InfoCert, secondo le modalità indicate dal presente manuale operativo, sono Certificati per firma elettronica avanzata o sigillo elettronico avanzato ai sensi del CAD e dell'articolo 26 ovvero articolo 36 del Regolamento eIDAS.

Il certificato emesso dalla CA sarà usato per verificare la firma elettronica avanzata o del sigillo elettronico del Soggetto 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 nei contratti, e comunque in violazione dei limiti d'uso e di valore (*key usage, extended key usage, user notice*) indicati nel certificato.

## **1.5 Amministrazione del Manuale Operativo**

### **1.5.1 Amministratore del Manuale Operativo**

### **1.5.2 Contatti**

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo

documento. Domande, reclami, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte ai seguenti recapiti:

InfoCert S.p.A.

Responsabile del Servizio di Certificazione Digitale

Piazza Luigi da Porto n.3

35131 Padova

Telefono: 06 836691

Call Center Firma Digitale: consultare il link <https://help.infocert.it/contatti/> per maggiori dettagli

Web: <https://www.firma.infocert.it>, <https://www.infocert.it>

e-mail: [firma.digitale@legalmail.it](mailto:firma.digitale@legalmail.it)

Il Soggetto o il Richiedente possono richiedere copia della documentazione a lui relativa, compilando e inviando il modulo disponibile sul sito [www.firma.infocert.it](http://www.firma.infocert.it) e seguendo la procedura ivi indicata. La documentazione verrà inviata in formato elettronico all'indirizzo di email indicato nel modulo.

### **1.5.3 Soggetti responsabili dell'approvazione del Manuale Operativo**

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle policies, dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dal Responsabile Legale, dal Responsabile Regulatory e approvato dalla Direzione Aziendale.

### **1.5.4 Procedure di approvazione**

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

## **1.6 Definizioni e acronimi**

### **1.6.1 Definizioni**

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal Regolamento eIDAS [1] e dal CAD [2] 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.

<b>Termine</b>	<b>Definizione</b>
<b>Autocertificazione</b>	È la dichiarazione, rivolta alla CA, effettuata personalmente dal soggetto che risulterà Soggetto del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità con assunzione delle responsabilità stabilite per legge.
<b>Conformity Assessment Body (Organismo di valutazione della conformità) (CAB)</b>	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.
<b>Conformity Assessment Report (Relazione di valutazione della conformità) (CAR)</b>	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]).
<b>Card Management System (CMS)</b>	Strumento di autenticazione, identificazione, raccolta e conservazione dei dati relativi ai Soggetti o ai Richiedenti
<b>certificato di firma elettronica</b>	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])
<b>certificato qualificato di firma elettronica</b>	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (cfr eIDAS [1])
<b>chiave di certificazione o chiave di root</b>	Coppia di chiavi crittografiche utilizzate dalla CA per firmare i certificati e le liste dei certificati revocati o sospesi

<b>chiave privata</b>	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Soggetto, mediante la quale si appone la firma elettronica sul documento informatico
<b>chiave pubblica</b>	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma elettronica apposta sul documento informatico dal Soggetto
<b>Cliente</b>	Soggetto con cui InfoCert ha formalizzato un contratto di fornitura di servizi dietro pagamento di corrispettivo
<b>codice di emergenza (ERC)</b>	Codice di sicurezza consegnato al Soggetto per inoltrare la richiesta di sospensione di un certificato sui portali del TSP
<b>convalida</b>	Il processo di verifica e conferma della validità di una firma (cfr eIDAS [1])
<b>dati di convalida</b>	Dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1])
<b>dati di identificazione personale</b>	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr eIDAS [1])
<b>dati per la creazione di una firma elettronica</b>	I dati unici utilizzati dal firmatario per creare una firma elettronica (cfr eIDAS [1])
<b>dispositivo per la creazione di una firma elettronica</b>	Un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1])
<b>dispositivo per la creazione di una firma elettronica qualificata (SSCD – secure system creation device o QSCD)</b>	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
<b>documento elettronico</b>	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1])
<b>firma automatica</b>	Particolare procedura informatica di firma elettronica eseguita previa autorizzazione del

	sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
<b>firma digitale (digital signature)</b>	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Soggetto tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (cfr CAD [2])
<b>firma elettronica</b>	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (cfr eIDAS [1])
<b>firma elettronica avanzata</b>	Una firma elettronica che soddisfa i requisiti di cui all'articolo 26 del Regolamento eIDAS (cfr eIDAS [1])
<b>firma elettronica qualificata</b>	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr eIDAS [1])
<b>firmatario</b>	Una persona fisica che crea una firma elettronica (cfr eIDAS [1])
<b>giornale di controllo</b>	Consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [5].
<b>identificazione elettronica</b>	Il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica (cfr eIDAS [1])
<b>lista dei certificati revocati o sospesi (Certificate Revocation List - CRL)</b>	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.
<b>manuale operativo (certificate practice statement)</b>	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.
<b>mezzi di identificazione elettronica</b>	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr eIDAS [1])
<b>Online Certificate Status Protocol (OCSP)</b>	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
<b>OTP - One Time Password:</b>	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 Soggetto in un momento immediatamente antecedente all'apposizione della firma elettronica. Può essere basato su dispositivi hardware o su procedure software.
<b>parte facente affidamento sulla certificazione</b>	Una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario (cfr eIDAS [1])
<b>prestatore di servizi fiduciari</b>	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])
<b>prestatore di servizi fiduciari qualificato</b>	Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr eIDAS [1])
<b>prodotto</b>	Un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari (cfr eIDAS [1])

<b>pubblico ufficiale</b>	Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche
<b>registro pubblico (Directory)</b>	Il Registro pubblico è un archivio che contiene: tutti i certificati emessi dalla CA per i quali sia stata richiesta dal Soggetto la pubblicazione; la lista dei certificati revocati e sospesi (CRL).
<b>revoca o sospensione di un certificato:</b>	È l'operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
<b>ruolo</b>	Il termine Ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del Soggetto, 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.
<b>servizio fiduciario</b>	Un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: 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 creazione, verifica e convalida di certificati di autenticazione di siti web; o conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1])
<b>servizio fiduciario qualificato</b>	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1])
<b>Tempo Universale Coordinato (Coordinated Universal Time):</b>	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
<b>validazione temporale elettronica</b>	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])

<b>validazione temporale elettronica qualificata</b>	Una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS (cfr eIDAS [1])
<b>webCam</b>	Videocamera di ridotte dimensioni, destinata a trasmettere immagini in streaming via Internet e catturare immagini fotografiche. Collegata a un PC o integrata in dispositivi mobile è utilizzata per chat video o per videoconferenze.

### 1.6.2 Acronimi e abbreviazioni:

<b>Acronimo</b>	<b>Significato</b>
<b>AgID</b>	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari;
<b>CA</b>	Certification Authority
<b>CAB</b>	Conformity Assessment Body – Organismo di valutazione della conformità
<b>CAD</b>	Codice dell'Amministrazione Digitale
<b>CAR</b>	Conformity Assessment Report – Relazione di valutazione della conformità
<b>CC</b>	Common Criteria
<b>CIE</b>	Carta di Identità Elettronica;
<b>CMS</b>	Card Management System
<b>CNS – TS-CNS</b>	Carta Nazionale dei Servizi Tessera Sanitaria – Carta Nazionale dei Servizi
<b>CRL</b>	Certificate Revocation List;
<b>DMZ</b>	Demilitarized Zone
<b>DN</b>	Distinguish Name
<b>EAL</b>	Evaluation Assurance Level
<b>eID</b>	Electronic Identity
<b>eIDAS</b>	Electronic Identification and Signature Regulation
<b>ERC</b>	Emergency Request Code

<b>ETSI</b>	European Telecommunications Standards Institute;
<b>FIPS</b>	Federal Information Processing Standard
<b>HSM</b>	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;
<b>http</b>	HyperText Transfer Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>IR</b>	Incaricato alla Registrazione
<b>ISO</b>	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione;
<b>ITU</b>	International Telecommunication Union: fondata nel 1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
<b>IUT</b>	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;
<b>LDAP</b>	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati;
<b>LoA</b>	Level of Assurance
<b>NTR Code</b>	National Trade Register Code
<b>OID</b>	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;
<b>OTP</b>	OneTime Password
<b>PEC</b>	Posta Elettronica Certificata

<b>PIN</b>	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Soggetto per accedere alle funzioni del dispositivo stesso;
<b>PKCS</b>	Public-Key Cryptography Standards
<b>PKI</b>	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
<b>RA</b>	Registration Authority – Autorità di Registrazione
<b>RFC</b>	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
<b>RSA</b>	Deriva dalle iniziali degli inventori dell'algoritmo: Rivest, Shamir, Adleman
<b>SGSI</b>	Sistema di Gestione per la Sicurezza delle Informazioni
<b>SPID</b>	Sistema Pubblico di Identità Digitale
<b>SSCD – QSSCD</b>	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
<b>TIN</b>	Tax Identification Number
<b>URL</b>	Uniform Resource Locator
<b>VAT Code</b>	Value Added Tax Code
<b>X509</b>	Standard ITU-T per le PKI
<b>X500</b>	Standard ITU-T per i servizi LDAP e directory

## **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 della Certification Authority (cfr. § 1.5.2).

#### **2.2.2 Pubblicazione dei certificati**

Non è prevista la possibilità di rendere pubblici i certificati emessi nell'ambito del presente Manuale Operativo.

#### **2.2.3 Pubblicazione delle liste di revoca e sospensione**

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP o con protocollo http all'indirizzo riportato nell'attributo "CRL Distribution Points" del certificato. 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 il protocollo LDAP e/o HTTP.

La CA 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 ove indicato al par. 1.5.2 ogni qualvolta ci siano delle modifiche significative.

#### **2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione**

Le CRLs vengono pubblicate ogni ora ove indicato al par. 2.2.3.

### **2.4 Controllo degli accessi agli archivi pubblici**

Le informazioni relative ai certificati pubblicati, alle CRLs e i manuali operativi sono

pubbliche, la CA non ha messo restrizione all'accesso in lettura e ha attuato tutte le contromisure per scongiurare modifiche/cancellazioni non autorizzate.

## 3 IDENTIFICAZIONE E AUTENTICAZIONE

### 3.1 Denominazione

#### 3.1.1 Tipi di nomi

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

#### 3.1.2 Necessità che il nome abbia un significato

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

#### 3.1.3 Anonimato e pseudonimia dei richiedenti

Solo in caso di identificazione secondo la modalità 1\_LiveID (vedi 3.2.3.1) è facoltà del Soggetto richiedere alla CA che il certificato riporti uno pseudonimo in luogo dei propri dati reali. La CA conserverà le informazioni relative alla reale identità della persona per un numero di anni dall'emissione del certificato stesso come stabilito contrattualmente.

#### 3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert 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:

- il Codice Fiscale per i cittadini italiani;
- il TIN – Tax Identification Number per i cittadini stranieri. Il TIN può essere stato assegnato dalle autorità del Paese di cui il Soggetto è cittadino ovvero dal Paese in cui ha la sede l'organizzazione in cui esso lavora.

In assenza di Codice Fiscale o TIN, nel certificato potrà essere inserito un codice identificativo tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento.

Nel caso di persona giuridica, per garantire l'univocità del soggetto, nel certificato deve essere indicato il nome dell'organizzazione e un codice identificativo univoco:

- la Partita IVA o il Numero di Registro Imprese per le persone giuridiche italiane,
- i codici VAT (Value Added Tax Code) o NTR (National Trade Register) per le

persone giuridiche.

### 3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

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

La CA non fa verifiche sull'utilizzo di marchi, e può rifiutarsi di 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 Soggetto o del Richiedente al momento della richiesta di rilascio del certificato.

La procedura di identificazione comporta che il Soggetto 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

InfoCert 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 Soggetto 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 LiveID	<ul style="list-style-type: none"> <li>• Certification Authority (CA)</li> <li>• Registration Authority (RA)</li> <li>• Incaricato alla Registrazione</li> <li>• Pubblico Ufficiale</li> <li>• Datore di Lavoro per la identificazione dei propri</li> </ul>	n/a

	dipendenti, collaboratori, agenti	
<b>2 AMLID</b>	<ul style="list-style-type: none"> <li>Soggetti destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive normative comunitarie di esecuzione</li> </ul>	n/a
<b>3 SignID</b>	<ul style="list-style-type: none"> <li>Certification Authority (CA)</li> <li>Registration Authority (RA)</li> <li>Incaricato alla Registrazione</li> </ul>	Utilizzo di una firma elettronica qualificata emessa da un Prestatore di Servizi Fiduciari Qualificato
<b>4 AutID</b>	<ul style="list-style-type: none"> <li>Certification Authority (CA)</li> <li>Registration Authority (RA)</li> <li>Incaricato alla Registrazione</li> </ul>	<ul style="list-style-type: none"> <li>Utilizzo di un dispositivo CNS o TS-CNS in corso di validità</li> <li>Utilizzo di un dispositivo CIE in corso di validità</li> <li>Utilizzo di una identità SPID, in corso di validità e emessa da un Gestore di Identità Digitale SPID</li> <li>Utilizzo di una eID in corso di validità emessa da un Prestatore di Servizi Fiduciari</li> <li>Utilizzo di una identità proveniente da altri sistemi di identificazione</li> </ul>

		<p>informatica ritenuti conformi</p> <ul style="list-style-type: none"> <li>• Utilizzo di un sistema basato sulla raccolta di dati biometrici</li> </ul>
<b>5 Videoid</b>	<p>Certification Authority (CA) Registration Authority (RA)</p> <ul style="list-style-type: none"> <li>• Incaricato alla Registrazione</li> </ul>	n/a
<b>6 SelfID</b>	<p>Certification Authority (CA) Registration Authority (RA) Incaricato alla Registrazione</p>	n/a

### 3.2.3.1 Riconoscimento effettuato secondo la modalità 1 - LiveID

La modalità di identificazione **LiveID** prevede un incontro di persona tra il Soggetto, che deve essere maggiorenne, e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti d'identificazione in corso di validità<sup>1</sup>. Il Soggetto deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato ad eseguire il riconoscimento. I soggetti privi di codice fiscale italiano devono esibire il documento contenente il TIN<sup>2</sup> o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. In mancanza di tale codice identificativo potrà essere utilizzato il numero del passaporto.

L'identificazione già eseguita dal datore di lavoro, ai fini della stipula del contratto di lavoro, è considerata valida dalla CA in conformità con la seguente modalità di riconoscimento:

<sup>1</sup> Per l'Italia sono i documenti previsti dal DPR 445/2000 e s.m.i. (Testo Unico Documentazione Amministrativa). I titolari con cittadinanza diversa da quella italiana, ai fini dell'identificazione esibiscono in originale uno dei seguenti documenti d'identificazione:

- passaporto,
- carta di identità italiana (se cittadini europei).

La CA si riserva la facoltà di accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, sulla base della analisi delle caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione dei documenti stessi da parte della Autorità Emittenti

<sup>2</sup> Tax Identification Number, è il numero di identificazione nazionale assegnato dai paesi della Unione Europea ai propri cittadini, con finalità di identificazione nel servizio fiscale nazionale

- l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia;
- l'identificazione eseguita dal datore di lavoro dei già dipendenti in stato di pensione, che continuano ad accedere ai portali e/o ai locali aziendali per esigenze ricreative, o di agevolazioni su beni e servizi, previsti dagli accordi aziendali.

I dati di registrazione per la modalità di identificazione LiveID sono conservati dalla CA in formato analogico o in formato elettronico.

### **3.2.3.2 Riconoscimento effettuato secondo la modalità 2 - AMLID**

Nella **modalità 2 - AMLID** la CA si avvale dell'identificazione eseguita da uno dei soggetti destinatari degli obblighi di Identificazione e Adeguata Verifica, ai sensi delle normative tempo per tempo vigenti, di recepimento della Direttiva UE 2015/849, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive ulteriori normative comunitarie di esecuzione.

Con specifico riferimento al contesto italiano, i dati utilizzati per il riconoscimento sono rilasciati dal Soggetto ai sensi del D.Lgs. 90/20017 e s.m.i. [6], a norma del quale i clienti sono tenuti a fornire - sotto la propria responsabilità - tutte le informazioni necessarie e aggiornate per consentire ai Soggetti destinatari degli Obblighi elencati nella predetta norma, di adempiere agli obblighi di identificazione della clientela. I soggetti destinatari degli obblighi acquisiscono i dati in base alle procedure definite in autonomia nel rispetto di quanto previsto dal D.Lgs. 90/20017 e s.m.i., ovvero alle analoghe procedure adottate secondo le norme antiriciclaggio vigenti alla data del riconoscimento (anche se in epoca anteriore al presente Manuale).

Questa modalità di identificazione prevede il conferimento, da parte della CA, di un mandato con rappresentanza al soggetto destinatario degli obblighi, che agisce quindi da RA. I dati identificativi del Soggetto raccolti all'atto del riconoscimento sono conservati dalla CA di norma in modalità elettronica e possono essere conservati anche in modalità analogica.

### **3.2.3.3 Riconoscimento effettuato secondo la modalità 3 - SignID**

Nella **modalità 3 SignID** la CA InfoCert si basa sul riconoscimento già effettuato da un'altra CA che emette certificati qualificati. Il Soggetto è già in possesso di un certificato ancora in corso di validità, che utilizza nei confronti di InfoCert. I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

### **3.2.3.4 Riconoscimento effettuato secondo la modalità 4 - AUTID**

Nella **modalità 4 AutID** la CA si basa sul riconoscimento già effettuato da autorità

pubbliche o private per l'emissione di:

- CNS (Carta nazionale dei Servizi), TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi) o CIE (Carta di Identità Elettronica) in Italia;
- Carta di Identità Elettronica di un paese Europeo,
- Gestore di Identità Digitale SPID (Sistema Pubblico di Identità Digitale SPID) o altro Identity Provider eID eIDAS;
- Un mezzo di identificazione elettronica pre-esistente, non notificato ed emesso da una autorità pubblica o un soggetto privato, a condizione che fornisca una garanzia equivalente alla presenza fisica sotto il profilo dell'affidabilità.
- Sistema di identificazione biometrico.

Il Soggetto deve essere quindi in possesso di un dispositivo sicuro con un certificato ancora in corso di validità, ovvero di una identità digitale eIDAS, con la quale si autentica ai sistemi della CA o della RA che ne accerta così l'identità.

Si considera coerente con la presente modalità di identificazione l'utilizzo di una identità proveniente da altri sistemi di identificazione informatica ritenuti conformi, il cui uso sia stato regolamentato attraverso il contratto tra CA e Richiedente.

Sono ritenuti mezzi validi ai fini dell'autenticazione anche modalità biometriche eventualmente messe a disposizione da parte del Richiedente o dalla RA. Questo consente l'identificazione attraverso elementi biometrici come la firma grafometrica, impronte digitali, autenticazione vocale o altro.

I dati di registrazione sono conservati, in questi casi, esclusivamente in formato elettronico.

### **3.2.3.5 Riconoscimento effettuato secondo la modalità 5 - VideoID**

Nella **modalità 5 VideoID** è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphome, tablet, etc.), una webcam e un sistema audio funzionante.

L'Incaricato alla Registrazione verifica l'identità del Soggetto o del Richiedente tramite il riscontro con uno o più documenti di riconoscimento in corso di validità, purché muniti di fotografia recente e riconoscibile.

Per ragioni di sicurezza e procedure anti-frode, il tipo di documenti accettati da questa modalità è limitato ai documenti di identità maggiormente diffusi (come ad esempio la

carta di identità, la patente, il passaporto)<sup>3</sup>. È facoltà dell'Incaricato alla Registrazione escludere l'ammissibilità del documento utilizzato dal Soggetto o dal Richiedente se ritenuto carente delle caratteristiche minime sufficienti per assicurare la validità del documento. I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

È facoltà della CA o della RA identificare la clientela attraverso una modalità video asincrona: ossia dando facoltà al Soggetto o al Richiedente in una prima fase di inviare le evidenze a supporto della verifica dell'identità attraverso il caricamento di un video e solo successivamente verificare queste evidenze raccolte. Durante questo video il Soggetto sarà invitato a seguire le istruzioni legate all'identificazione che non verrà più guidata da un operatore ma da uno script o altro strumento informatico. Dopodiché la verifica sulla bontà del video e sulla congruità del contenuto a quanto impartito dalla procedura informatica, verrà svolto in un momento successivo da personale della CA o della RA.

### 3.2.3.6 Riconoscimento asincrono unattended

Nella **modalità 6 SelfID** l'identificazione avviene senza la presenza contestuale dell'Incaricato alla Registrazione e del Soggetto o Richiedente all'interno della sessione audiovideo. In questa configurazione il Soggetto effettua in autonomia la sessione di riconoscimento, caricando il proprio documento d'identità e seguendo le istruzioni per una procedura automatica di ripresa del suo volto (c.d. "video-selfie"), durante la quale compie alcune azioni casuali di rafforzamento, secondo le istruzioni della procedura predisposte dalla CA. Quest'ultima si avvale di una tecnologia che resituisce un indice di compatibilità tra il Soggetto e i documenti presentati: qualora l'indice di compatibilità (c.d. "scoring") non raggiunga valori sufficienti, il processo non va a buon fine e il Soggetto deve ripetere il riconoscimento. Alternativamente, può essere prevista la presenza di un back-office che effettui verifiche asincrone e raccolga le ulteriori evidenze eventualmente necessarie al buon fine del riconoscimento.

Per ragioni di sicurezza e procedure anti-frode, il tipo di documenti accettati da questa modalità è limitato ai documenti di identità maggiormente diffusi (come ad esempio la carta di identità, la patente, il passaporto)<sup>4</sup>.

---

<sup>3</sup> La CA si riserva la facoltà di accettare ulteriori tipologie di documenti di identità, ovvero documenti emessi da autorità di Paesi appartenenti alla Unione Europea, sulla base della analisi delle caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione dei documenti stessi da parte della Autorità Emittenti.

<sup>4</sup> La CA si riserva la facoltà di accettare ulteriori tipologie di documenti di identità, ovvero documenti emessi da autorità di Paesi appartenenti alla Unione Europea, sulla base della analisi delle caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione dei documenti stessi da parte della Autorità Emittenti.

### **3.2.4 Identificazione della persona giuridica**

La richiesta di certificato per persona giuridica deve essere effettuata da una persona fisica identificata in una delle modalità descritte sopra (cfr § 3.2.3).

Deve inoltre presentare la documentazione aggiornata relativa agli estremi della persona giuridica e la documentazione che attesti il titolo della persona fisica ad avanzare la richiesta per conto della persona giuridica.

### **3.2.5 Informazioni del Soggetto o del Richiedente non verificate**

Il Soggetto può ottenere l'inserimento nel certificato di informazioni relative sui propri Titoli e/o abilitazioni Professionali.

Questi ulteriori attributi, se utilizzati all'interno del circuito SPID, devono essere comunicati da parte dell'Attribute Provider abilitato a questo tipo di attestazioni.

### **3.2.6 Validazione dell'autorità**

La CA ovvero la RA verificano le informazioni richieste, definite nel paragrafo 4.2.1, per l'identificazione e validano la richiesta.

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

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

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

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (validity) con gli attributi "valido dal" (*not before*) e "valido fino al" (*not after*). Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

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

## **3.4 Identificazione e autenticazione per le richieste di revoca o**

## **sospensione**

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

### **3.4.1 Richiesta da parte del Soggetto**

Il soggetto può richiedere la revoca o sospensione compilando e sottoscrivendo anche in modalità elettronica il modulo presente sul sito della CA.

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

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

Nel caso in cui il Soggetto sia una persona giuridica, la richiesta di sospensione o revoca deve essere eseguita da un legale rappresentante o un soggetto munito di apposita procura.

### **3.4.2 Richiesta da parte del Richiedente**

Il Richiedente che richiede la revoca o sospensione del certificato del Soggetto si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dalla CA. La richiesta dovrà essere inoltrata con le modalità indicate ai paragrafi 4.9.3.2 o 4.9.15.2. La CA si riserva di individuare ulteriori modalità di inoltro della richiesta, di revoca o sospensione del Richiedente o del Terzo Interessato in apposite convenzioni da stipulare con lo stesso.

## 4 OPERATIVITÀ

### 4.1 Richiesta del certificato

#### 4.1.1 Chi può richiedere un certificato

Il certificato per una persona fisica può essere richiesto da:

- Il Soggetto,
  - rivolgendosi direttamente alla CA al sito [www.firma.infocert.it](http://www.firma.infocert.it) o [www.infocert.it](http://www.infocert.it) o al sito [www.infocert.digital](http://www.infocert.digital)
  - rivolgendosi a una Registration Authority
- Il Richiedente per conto del Soggetto
  - rivolgendosi direttamente alla CA mediante il sito [www.firma.infocert.it](http://www.firma.infocert.it) o [www.infocert.it](http://www.infocert.it) o al sito [www.infocert.digital](http://www.infocert.digital) stipulando un accordo commerciale con la CA
  - rivolgendosi a una Registration Authority

Il certificato per una persona giuridica può essere richiesto da:

- Il Richiedente che rappresenta la persona giuridica
  - rivolgendosi direttamente alla CA mediante il sito [www.firma.infocert.it](http://www.firma.infocert.it) o [www.infocert.it](http://www.infocert.it) o il sito [www.infocert.digital](http://www.infocert.digital) o stipulando un accordo commerciale con la CA
  - rivolgendosi a specifiche Registration Authority appositamente istruite per emettere certificati di questo tipo.

#### 4.1.2 Processo di registrazione e responsabilità

Il processo di registrazione comprende: la richiesta da parte del Soggetto, 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 Soggetto 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. Quando il Soggetto è una persona

- giuridica, tali responsabilità ricadono sul legale rappresentante o soggetto munito di apposita procura, che richiede il certificato;
- Il Richiedente, ove presente, ha la responsabilità di informare il Soggetto, per conto del quale sta richiedendo il certificato, sugli obblighi derivanti dal certificato, di fornire le informazioni corrette e veritiere sull'identità del Soggetto, 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 Soggetto 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.

Nel caso in cui le chiavi siano generate in un dispositivo del Soggetto, il Richiedente deve inviare anche la richiesta in formato PKCS#10 firmata dal richiedente stesso.

## **4.2 Elaborazione della richiesta**

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

- prendere visione del presente Manuale Operativo, della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel paragrafo 3;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

### **4.2.1 Informazioni che il Soggetto deve fornire**

#### **4.2.1.1 Persona fisica**

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

- Cognome e Nome;
- Data e luogo di nascita;
- Codice fiscale o analogo codice identificativo (TIN);

- Indirizzo di residenza;
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- e-mail per l'invio delle comunicazioni dalla CA al Soggetto;
- numero di telefonia mobile per la trasmissione della OTP ove fosse questa la tecnologia OTP adottata.

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

Nel caso in cui la persona fisica volesse certificare le proprie coppie di chiavi, il richiedente deve fornire anche il file in formato PKCS#10 della richiesta firmata dal Richiedente.

#### **4.2.1.2 Persona giuridica**

Per la richiesta di un certificato per persona giuridica il Richiedente, individuato nel legale rappresentante o persona fisica dotata di procura, deve fornire obbligatoriamente le seguenti informazioni:

- Cognome e Nome del Richiedente;
- Codice fiscale o analogo codice identificativo del Richiedente (TIN);
- Estremi del documento di riconoscimento presentato per l'identificazione del Richiedente, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- e-mail per l'invio delle comunicazioni dalla CA al Richiedente;
- Nome del Soggetto persona giuridica;
- Partita IVA ovvero numero di Registro Imprese per i Soggetti italiani, VAT code ovvero NTR per Soggetti stranieri.

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

Nel caso in cui la persona giuridica volesse certificare le proprie coppie di chiavi, il richiedente deve fornire anche il file in formato PKCS#10 della richiesta firmata dal Richiedente

Le informazioni fornite sono memorizzate negli archivi della CA (fase di registrazione) e saranno la base per la generazione del certificato.

#### **4.2.2 Esecuzione delle funzioni di identificazione e autenticazione**

Durante la fase di registrazione iniziale e raccolta della richiesta di registrazione e

certificazione vengono consegnati al Soggetto o al Richiedente, legale rappresentante della persona giuridica, i codici di sicurezza che gli consentono sia di procedere alla attivazione del dispositivo di firma o della procedura di firma, se remota, e alla eventuale richiesta di sospensione del certificato (codice ERC o codice analogo, se previsto dal contratto). I codici di sicurezza sono consegnati in busta cieca ovvero, se elettronici, trasmessi all'interno di file cifrati se elettronici ovvero, in alcuni casi, coincidono con codici già in possesso del Soggetto.

La CA può prevedere che il PIN di firma sia scelto in autonomia dal Soggetto o dal Richiedente legale rappresentante della persona giuridica; in tali casi è onere del Soggetto o del Richiedente ricordare il PIN.

### **4.2.3 Approvazione o rifiuto della richiesta del certificato**

Dopo la registrazione iniziale la CA o la RA possono rifiutarsi di portare a termine l'emissione del certificato di sottoscrizione in caso di assenza o incompletezza di informazioni, verifiche di coerenza e consistenza delle informazioni fornite, verifiche anti-frode, dubbi sull'identità del Soggetto 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 Soggetto (o Richiedente) e dalla eventuale necessità di raccogliere ulteriori informazioni ovvero di consegnare fisicamente il dispositivo.

## **4.3 Emissione del certificato**

### **4.3.1 Azioni della CA durante l'emissione del certificato**

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

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

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

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

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

Il Soggetto o il Richiedente si autenticano 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.

#### **4.3.1.3 Emissione del certificato attraverso un sistema di Card Management System**

La coppia di chiavi crittografiche viene generata dalla RA direttamente sui dispositivi utilizzando un sistema di Card Management System autenticato. Il sistema gestisce il ciclo di vita completo del dispositivo crittografico, inviando alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10 firmata digitalmente, attraverso 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 è inviato su canale sicuro all'interno del dispositivo.

#### **4.3.1.4 Emissione del certificato a persona giuridica**

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

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

Nel caso in cui la coppia di chiavi sia generata nel dispositivo HSM del Soggetto, questi dovrà inviare il PKCS#10 firmato e 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**

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

### **4.3.3 Attivazione**

#### **4.3.3.1 Attivazione del dispositivo di firma (smartcard o token)**

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

#### **4.3.3.2 Attivazione del dispositivo di firma remota (HSM)**

Per attivare il dispositivo di firma remota il Soggetto, ovvero il Richiedente in caso di persona giuridica, sceglie il PIN di firma, quantità di sicurezza riservata la cui custodia e tutela è posta esclusivamente in capo al Soggetto stesso, che viene confermato con l'inserimento della OneTime Password ricevuta via SMS, ovvero generata sul token o la token-app associata al certificato.

In alcuni casi, l'attivazione della firma remota può essere eseguita utilizzando una o più componenti di un sistema di autenticazione gestito dalla RA. In tale ipotesi la CA provvede a verificare preventivamente la rispondenza dei requisiti di sicurezza del sistema, assicurandosi che tale sistema garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del Titolare, anche attraverso audit periodici. Gli aspetti di responsabilità sono regolati contrattualmente.

## **4.4 Accettazione del certificato**

### **4.4.1 Comportamenti concludenti di accettazione del certificato**

n/a

### **4.4.2 Pubblicazione del certificato da parte della Certification Authority**

Al buon esito della procedura di certificazione, il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico.

### **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 Soggetto**

Il Soggetto deve custodire in maniera sicura il dispositivo di firma, se presente, ovvero

gli strumenti di autenticazione per la firma remota; deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo. Deve garantire la protezione della segretezza e la conservazione degli eventuali codici di emergenza necessari alla sospensione del certificato, deve utilizzare il certificato per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.

Non deve apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato e non deve apporre firme elettroniche avvalendosi di certificato emesso da CA revocata.

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

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

#### **4.5.3 Limiti d'uso e di valore**

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

È possibile emettere certificati di firma elettronica avanzata e di sigillo elettronico avanzato a solo scopo di test inserendo il seguente limite d'uso:

- L'utilizzo del certificato è limitato alla sottoscrizione di documenti per finalità di test. The use of the certificate is limited to the signature of documents for test purpose.

### **4.6 Rinnovo del certificato**

#### **4.6.1 Motivi per il rinnovo**

Il rinnovo consente di ottenere un nuovo certificato.

#### **4.6.2 Chi può richiedere il rinnovo**

Il Soggetto può richiedere il rinnovo del certificato prima della sua scadenza solo se non è stato revocato; oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla richiesta di un nuovo certificato.

La procedura di rinnovo si applica esclusivamente a certificati emessi da InfoCert.

Il rinnovo di certificato per firma automatica non è previsto e si dovrà procedere ad una nuova emissione.

Il rinnovo di un certificato emesso a una persona giuridica non è previsto, si dovrà procedere ad una nuova emissione.

### **4.6.3 Elaborazione della richiesta di rinnovo del certificato**

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

### **4.7 Riemissione del certificato**

n/a

### **4.8 Modifica del certificato**

n/a

### **4.9 Revoca e sospensione del certificato**

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

#### **4.9.1 Motivi per la revoca**

Le condizioni per cui deve essere effettuata la richiesta di revoca sono le seguenti:

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
  - sia stato smarrito il dispositivo sicuro di firma che contiene la chiave;
  - sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN) oppure, per i certificati di firma remota, sia stato compromesso o smarrito il dispositivo OTP;
  - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave.

2. il Soggetto non riesce più ad utilizzare il dispositivo sicuro di firma in suo possesso, ad esempio per un guasto;
3. si verifica un cambiamento dei dati del Soggetto presenti nel certificato, ivi compresi quelli relativi al Ruolo, tale da rendere detti dati non più corretti e/o veritieri;
4. termina il rapporto tra il Soggetto e la CA, ovvero tra il Richiedente e la CA;
5. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

#### **4.9.2 Chi può richiedere la revoca**

La revoca può essere richiesta dal Soggetto in qualsiasi momento 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 Soggetto**

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

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

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

##### **4.9.3.2 Revoca richiesta dal Richiedente o dal Terzo Interessato**

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

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

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

#### **4.9.3.3 Revoca su iniziativa della Certification Authority**

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

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

#### **4.9.4 Periodo di grazia della richiesta di revoca**

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

#### **4.9.5 Tempo massimo di elaborazione della richiesta di revoca**

La richiesta di revoca viene evasa e il nuovo stato del certificato viene pubblicato entro 24 (ventiquattro) ore, fatto salvo il caso in cui vi siano dei dubbi sull'autenticità della richiesta stessa. In questi casi la CA si riserva ulteriori verifiche, ad esempio, per accertare l'identità del richiedente. In quest'ultimo caso, si provvede alla sospensione del certificato in attesa di eseguire ulteriori accertamenti sull'autenticità della richiesta ricevuta.

#### **4.9.6 Requisiti per la verifica della revoca**

n/a

#### **4.9.7 Frequenza di pubblicazione della CRL**

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

forzare un'emissione non programmata della CRL (emissione straordinaria immediata), ad esempio nel caso in cui la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata). La CRL è emessa sempre integralmente. Il momento della pubblicazione della CRL viene attestata utilizzando quale riferimento temporale la data fornita dal sistema di Time Stamping Authority InfoCert e tale registrazione viene riportata sul giornale di controllo. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di revoca o sospensione. La CA si riserva la possibilità di pubblicare separatamente altre CRL, sottoinsiemi della CRL più generale, allo scopo di alleggerire il carico di rete. L'acquisizione e consultazione della CRL è a cura degli utenti. La CRL da consultare per lo specifico certificato è indicata nel certificato stesso secondo le norme vigenti.

#### **4.9.8 Latenza massima della CRL**

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

#### **4.9.9 Servizi online di verifica dello stato di revoca del certificato**

Oltre alla pubblicazione della CRL nei registri LDAP e http, InfoCert 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 ore 7 giorni la settimana.

#### **4.9.10 Requisiti servizi on line di verifica**

Si veda l'appendice A.

#### **4.9.11 Altre forme di revoca**

n/a

#### **4.9.12 Requisiti specifici rekey in caso di compromissione**

n/a

#### **4.9.13 Motivi per la sospensione**

La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il Soggetto, Il Richiedente o Terzo Interessato, la RA o la CA hanno acquisito elementi di dubbio sulla validità del certificato ovvero sull'identità del Soggetto o

- del Richiedente (ad es., per sospetto o denunciato furto o frode di identità);
3. siano insorti dubbi sulla sicurezza del dispositivo OTP, qualora presente;
  4. è necessaria un'interruzione temporanea della validità del certificato.

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

#### **4.9.14 Chi può richiedere la sospensione**

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

#### **4.9.15 Procedure per richiedere la sospensione**

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

##### **4.9.15.1 Sospensione richiesta dal Soggetto**

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

1. utilizzando la funzione di sospensione disponibile nel sito web della CA, comunicando i dati richiesti e utilizzando il codice di emergenza fornito in sede di emissione del certificato.
2. utilizzando (ove disponibile) la funzione di sospensione con OTP disponibile nel sito Web indicato nella documentazione contrattuale fornita all'atto della Registrazione.
3. telefonando al Call Center della CA e fornendo le informazioni richieste. In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una sospensione immediata del certificato per una durata di 10 (dieci) giorni solari in attesa della richiesta scritta del Soggetto; qualora la CA non riceva la richiesta sottoscritta entro il termine indicato, procede a riattivare il certificato tramite la Registration Authority, la quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione alla CA. Il Soggetto è tenuto a sottoscrivere la richiesta di sospensione e consegnarla alla RA o inviarla direttamente alla CA per posta ordinaria o PEC, corredata di una fotocopia di un documento di identità in corso di validità.

#### **4.9.15.2 Sospensione richiesta dal Richiedente o dal Terzo Interessato**

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

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

#### **4.9.15.3 Sospensione su iniziativa della CA**

La CA, salvo casi d'urgenza, comunica preventivamente al Soggetto l'intenzione di sospendere il certificato, fornendo il motivo della sospensione, la data di decorrenza e la data di termine. Queste ultime informazioni saranno in ogni caso comunicate al più presto al Soggetto.

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

### **4.9.16 Limiti al periodo di sospensione**

Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL). La riattivazione avviene nell'arco delle 24 (ventiquattro) ore successive alla data di termine della sospensione. Qualora il giorno di scadenza della sospensione coincida con il giorno di scadenza del certificato o sia a questa successivo, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

## **4.10 Servizi riguardanti lo stato del certificato**

### **4.10.1 Caratteristiche operative**

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

Le informazioni fornite dal servizio OCSP per i certificati sono aggiornate in tempo reale.

#### **4.10.2 Disponibilità del servizio**

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

#### **4.10.3 Caratteristiche opzionali**

##### **4.11 Disdetta dai servizi della CA**

Il rapporto del Soggetto 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

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

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui la CA gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Un estratto della politica di sicurezza InfoCert è disponibile facendone richiesta alla casella PEC [infocert@legalmail.it](mailto:infocert@legalmail.it).

### 5.1 Sicurezza fisica

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

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

#### 5.1.1 Posizione e costruzione della struttura

Il sito primario di erogazione InfoCert si trova presso la sede operativa di Padova. Il sito di Disaster Recovery è ubicato a Modena ed è connesso al Data Center sopra citato tramite un collegamento dedicato e ridondato su due circuiti diversi MPLS a 40 Gbit/s upgradabile fino a 100 Gbit/s.

All'interno di entrambi i siti sono stati ricavati dei locali protetti con dei più elevati livelli di sicurezza, sia fisici che logici, all'interno dei quali sono attestati gli apparati informatici

che costituiscono il cuore dei servizi di certificazione digitale, marcatura temporale, firma remota e automatica.

Per i servizi in continuità operativa con valori di RTO/RPO prossimi allo zero, alcune componenti dei servizi di CA relativi alla pubblicazione delle CRL e all'OCSP sono ospitati su infrastruttura cloud di fornitori terzi, rispettivamente, nella Regione Europa Francoforte e nella Regione Europa Irlanda. Per garantire inoltre la continuità operativa per la CA "InfoCert Advanced Electronic Signature CA 4" viene eseguita una copia cifrata dei dati su cloud AWS nella Regione Europa Milano.

I fornitori di cui InfoCert si avvale dispongono di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2013 e ISO/IEC 9001:2015. Per quanto riguarda l'infrastruttura cloud, i fornitori dispongono altresì delle certificazioni 27017:2015, 27018:2019.



Figura 1 - ubicazione sito di erogazione primario InfoCert e della Disaster Recovery

### 5.1.2 Accesso fisico

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

### **5.1.3 Impianto elettrico e di climatizzazione**

Il sito di erogazione di Padova è certificato rating 3 secondo la ANSI TIA 942.

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

L'infrastruttura preposta all'alimentazione include:

- Gruppi di continuità, dotati di accumulatori, in corrente alternata (UPS);
- Disponibilità di tensione alternata (220-380V AC);
- Armadi alimentati in ridondanza con linee protette e dimensionate per l'assorbimento concordato;
- Servizio di generatori di emergenza;
- Sistema di commutazione automatico e sincronizzazione fra generatori, rete e batterie (STS).

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

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

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

### **5.1.4 Prevenzione e protezione contro gli allagamenti**

La zona d'ubicazione dell'immobile non presenta rischi ambientali dovuti alla vicinanza ad installazioni "pericolose". Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica.

L'area che ospita gli apparati è al piano terreno in una posizione sopraelevata rispetto al livello della strada.

### **5.1.5 Prevenzione e protezione contro gli incendi**

È presente nel Data Center un impianto di rilevazione fumi gestito da centrale analogica indirizzata NOTIFIER con sensori ottici posizionati in ambiente e nel controsoffitto e sensori a campionamento d'aria installati sottopavimento e nelle canalizzazioni dell'aria.

L'impianto di rilevazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici ARGON IG-01.

Nel caso di intervento contemporaneo di due rivelatori nella stessa zona, è comandata la scarica di estinguente nella zona interessata.

Per ogni compartimento antincendio è previsto un impianto di estinzione dedicato.

Sono inoltre presenti mezzi estinguenti portatili in conformità alle leggi e normative vigenti.

Le canalizzazioni dell'aria primaria asservite alle sale apparati sono dotate, in corrispondenza degli attraversamenti dei compartimenti antincendio, di serrande tagliafuoco azionate dall'impianto automatico di rilevazione incendi.

### **5.1.6 Supporti di memorizzazione**

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp (FAS 8060). Per la parte SAN si è invece implementata un'infrastruttura 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**

InfoCert adotta un sistema di gestione certificato ISO 14001 per la gestione ambientale sostenibile. L'organizzazione adotta procedure interne per la cancellazione sicura dei dati dei dispositivi storage di classe enterprise tramite l'utilizzo di fornitori che ne garantiscono la cancellazione. Adotta inoltre un ciclo di gestione dei rifiuti conforme alle normative nazionali vigenti tramite procedure per la gestione e il monitoraggio del ciclo di vita dei rifiuti e si avvale esclusivamente di fornitori autorizzati al trasporto e al destino degli stessi.

### **5.1.8 Off-site backup**

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.

La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

## **5.3 Controllo del personale**

### **5.3.1 Qualifiche, esperienze e autorizzazioni richieste**

Effettuata la pianificazione annuale delle Risorse Umane, il Responsabile Funzione/Struttura Organizzativa identifica le caratteristiche e gli skill della risorsa da inserire (*job profile*). Successivamente, di concerto con il responsabile selezione, viene attivato il processo di ricerca e selezione.

### **5.3.2 Procedure di controllo delle esperienze pregresse**

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con il responsabile della selezione 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.

### **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 InfoCert ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici, con caratteristiche di affidabilità e riservatezza. Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

### **5.3.4 Frequenza di aggiornamento della formazione**

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

- Incontro con la Direzione Aziendale per la raccolta dei dati relativi alle esigenze formative necessarie per raggiungere gli obiettivi aziendali;
- Intervista ai Responsabili per la rilevazione delle esigenze formative specifiche delle proprie aree;
- Restituzione dei dati raccolti alla Direzione Aziendale per chiusura ed approvazione del Piano Formativo.

Entro il mese di febbraio il Piano Formativo così definito viene condiviso con i dipendenti.

### **5.3.5 Frequenza nella rotazione dei turni di lavoro**

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.

Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 (dieci) giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.

Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicinare nella reperibilità il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

### **5.3.6 Sanzioni per azioni non autorizzate**

Si fa riferimento al "CCNL Metalmeccanici e installazione impianti industria privata" per la procedura di irrogazione delle sanzioni ai dipendenti.

### **5.3.7 Controlli sul personale non dipendente**

L'accesso al personale non dipendente è regolato da una specifica policy aziendale.

### **5.3.8 Documentazione che il personale deve fornire**

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto in formato tessera per il badge di accesso ai locali. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti

riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette InfoCert.

## **5.4 Gestione del giornale di controllo**

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

### **5.4.1 Tipi di eventi memorizzati**

Vengono registrati eventi di sicurezza, avviamento e spegnimento, crash di sistema e guasti hardware, attività di firewall e router e tentativi di accesso sistema PKI.

Vengono conservati tutti i dati e documenti utilizzati in fase di identificazione e accettazione della domanda del richiedente: copia carta d'identità, contrattualistica, visura camerale ecc.

Vengono registrati gli eventi legati alla registrazione e al ciclo di vita dei certificati: le richieste di certificato e rinnovo, le registrazioni del certificato, la generazione, la diffusione, ed eventualmente la revoca/sospensione.

Vengono registrati tutti gli eventi riguardanti le personalizzazioni del dispositivo di firma.

Ogni evento viene salvato con data e ora di sistema dell'evento.

### **5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo**

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

### **5.4.3 Periodo di conservazione del giornale di controllo**

Il giornale di controllo viene conservato dalla CA, per un numero anni definito a livello contrattuale.

### **5.4.4 Protezione del giornale di controllo**

La protezione del giornale di controllo è garantita da Sistema di Conservazione dei documenti elettronici InfoCert, accreditato presso AgID secondo la normativa vigente.

### **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 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, a memorizzazione avviene nelle modalità previste dal sistema di conservazione norma InfoCert e descritto nel manuale del suddetto sistema.

#### **5.4.7 Notifica in caso di identificazione di vulnerabilità**

n/a

#### **5.4.8 Valutazioni di vulnerabilità**

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

### **5.5 Archiviazione dei verbali**

#### **5.5.1 Tipi di verbali archiviati**

Vengono redatti e archiviati verbali relativi ai più importanti eventi di una Certification Authority. I verbali vengono conservati per 20 (venti) anni dalla Certification Authority nel Sistema di Conservazione dei documenti InfoCert.

#### **5.5.2 Protezione dei verbali**

La protezione è garantita dal Sistema di Conservazione dei documenti InfoCert, accreditato in AgID.

#### **5.5.3 Procedure di backup dei verbali**

Il sistema di conservazione a norma attua una politica e procedura di backup, come previsto dal manuale 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, a memorizzazione avviene nelle modalità previste dal sistema di conservazione norma InfoCert e descritto nel manuale del suddetto sistema.

#### **5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi**

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema

di certificazione e dell'intera infrastruttura tecnica della CA.

## **5.6 Sostituzione della chiave privata della CA**

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

## **5.7 Compromissione della chiave privata della CA e disaster recovery**

### **5.7.1 Procedure per la gestione degli incidenti**

La CA ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27001. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente e inviato al Sistema di Conservazione InfoCert; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirante a eliminare le cause che possono aver dato luogo all'incidente, se sotto il controllo di InfoCert.

### **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.

Il 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.

InfoCert ha descritto la procedura da seguire in caso di compromissione della chiave, nell'ambito del SGSI certificato ISO 27001, dandone evidenza anche al CAB.

#### **5.7.4 Erogazione dei servizi di CA in caso di disastri**

InfoCert 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, InfoCert comunicherà questa intenzione all'Autorità di vigilanza (AgID) con un anticipo di almeno 60 (sessanta) giorni, indicando, eventualmente, il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione. Con pari anticipo InfoCert informa della cessazione delle attività tutti i possessori di certificati da esso emessi. Nella comunicazione, nel caso in cui non sia indicato un certificatore sostitutivo, sarà chiaramente specificato che tutti i certificati non ancora scaduti al momento della cessazione delle attività della CA saranno revocati.

## 6 CONTROLLI DI SICUREZZA TECNOLOGICA

### 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 Soggetti.

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 Soggetto

Le chiavi asimmetriche sono generate all'interno di un Dispositivo Sicuro per la Creazione della Firma SSCD ovvero QSCD utilizzando le funzionalità native offerte dai dispositivi stessi.

Nel caso in cui il dispositivo non sia messo a disposizione dalla CA, il richiedente deve assicurare che il dispositivo rispetti la normativa vigente, presentando apposita documentazione ed essendo soggetto a audit periodici.

### **6.1.2 Consegna della chiave privata al Richiedente**

La chiave privata è contenuta nel dispositivo crittografico, sia esso un SSCD o un QSCD. Con la consegna del dispositivo crittografico al Soggetto, questo entra in pieno possesso della chiave privata, che può utilizzare unicamente attraverso l'uso del PIN, di cui ha conoscenza esclusiva.

In caso di processo di registrazione svolto in presenza del Soggetto, il dispositivo è consegnato non appena sono generate le chiavi.

In caso di processo di registrazione svolto non in presenza del Soggetto, il dispositivo viene consegnato secondo le modalità condivise nel contratto, avendo sempre cura che il dispositivo e le informazioni per il suo utilizzo viaggino su canali differenti ovvero siano consegnati al Soggetto in due momenti temporalmente differenti.

### **6.1.3 Consegna della chiave pubblica alla CA**

n/a

### **6.1.4 Consegna della chiave pubblica agli utenti**

La chiave pubblica è contenuta nel certificato rilasciato solo al soggetto richiedente. Se il Richiedente ne fa richiesta, viene pubblicato anche nel registro pubblico, da dove può essere recuperato dall'Utente.

### **6.1.5 Algoritmo e lunghezza delle chiavi**

La coppia di chiavi asimmetriche di certificazione è generata all'interno di un dispositivo crittografico hardware di cui sopra.

Le chiavi di root CA che firmano l'emissione di nuovi certificati possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 4096 bit;

- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

Le chiavi del soggetto possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bits;

- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

### **6.1.6 Controlli di qualità e generazione della chiave pubblica**

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il § 6.2.1)

e garantiscono che la chiave pubblica sia corretta e randomica. La CA, prima di emettere il certificato, verifica che la chiave pubblica non sia già stata utilizzata.

## **6.1.7 Scopo di utilizzo della chiave**

### **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 ocpSigning.

### **6.1.7.1 Utilizzo chiave del Titolare**

Lo scopo di utilizzo della chiave del Titolare 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 InfoCert 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 in Europa.

Le smartcard e i moduli crittografici utilizzati da InfoCert per le chiavi di firma remota e automatica del Soggetto sono dispositivi crittografici sicuri.

### **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**

n/a

### **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 Soggetto o il Richiedente per conto di un soggetto giuridico è responsabile di proteggere la propria chiave privata con una password robusta per prevenire l'utilizzo non autorizzato. Per attivare la chiave privata, il Soggetto 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 InfoCert 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 o giuridica hanno validità non superiore ai 63 (sessantatre) mesi, compatibilmente con la robustezza degli algoritmi utilizzati.

## **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 (dodici) mesi.

## **6.6 Operatività sui sistemi di controllo**

InfoCert 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 per le attività EA:33-35.

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 InfoCert.

## **6.7 Controlli di sicurezza della rete**

InfoCert ha ideato, per il servizio di certificazione, un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi di firewalling e del protocollo SSL in modo da realizzare un canale sicuro tra gli Uffici di Registrazione ed il sistema di certificazione, nonché tra questo e gli amministratori/operatori.

I sistemi e le reti di InfoCert 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).

## **6.1 Controlli di sicurezza della rete**

Per la marcatura temporale occorre fare riferimento al manuale operativo ICERT-INDI-TSA presente sul sito del prestatore di servizi fiduciari InfoCert.



## 7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP

### 7.1 Formato del certificato

Nel certificato compaiono le informazioni indicate nella richiesta di certificazione.

Il formato del certificato prodotto è conforme al Regolamento eIDAS e alla Deliberazione CNIPA [9]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.

InfoCert utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.

In 0 il tracciato dei certificati di root e dei soggetti, siano essi persone fisiche o giuridiche.

#### 7.1.1 Numero di versione

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

#### 7.1.2 Estensioni del certificato

n/a

#### 7.1.3 OID dell'algoritmo di firma

L'algoritmo utilizzato per la firma dei certificati può essere scelto tra i seguenti:

sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(1 13549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]

ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]

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

ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

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

#### **7.2.1 Numero di versione**

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

#### **7.2.2 Estensioni della CRL**

Per le estensioni della CRL si veda l'APPENDICE A.

### **7.3 Formato dell'OCSP**

Per consentire di determinare lo stato di revoca del certificato senza fare richiesta alla CRL, InfoCert 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 InfoCert è conforme alla versione 1 del RFC6960.

#### **7.3.2 Estensioni dell'OCSP**

Per le estensioni dell'OCSP si veda l'APPENDICE A.

## 8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

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

### 8.1 Frequenza o circostanze per la valutazione di conformità

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

### 8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

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

### 8.3 Rapporti tra InfoCert e CAB

InfoCert presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 del 23/07/2014, sulla base di una valutazione di

conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319\_403 e UNI CEI EN ISO/IEC 17065:2012.

#### **8.4 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 la segnalerà a InfoCert richiedendo garanzia per la sua correzione. Il CAB può riservarsi di rieseguire l'audit dopo che la non conformità è stata sanata.

InfoCert 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 presso il sito [www.infocert.it](http://www.infocert.it), o presso le Registration Authority. La CA può stipulare accordi commerciali con le RA, e/o i Clienti 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 sospensione e revoca dei certificati

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

#### 9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili presso il sito [www.infocert.it](http://www.infocert.it), o presso le Registration Authority.

La CA può stipulare accordi commerciali con le RA, e/o i Clienti prevedendo tariffe specifiche.

#### 9.1.5 Politiche per il rimborso

Qualora il servizio venga acquistato da un soggetto che possa qualificarsi, sulla base della normativa, consumatore, questi ha il diritto di recedere dal contratto entro il termine di 14 giorni a decorrere dalla data di conclusione dello stesso, ottenendo il rimborso del prezzo pagato. Le istruzioni per l'esercizio del diritto di recesso e la richiesta di rimborso sono disponibili presso la sezione dedicata all'assistenza clienti del [www.infocert.it](http://www.infocert.it) o presso le RA.

### 9.2 Responsabilità finanziaria

#### 9.2.1 Copertura assicurativa

Il TSP InfoCert ha stipulato idonea polizza assicurativa per la copertura dei rischi dell'attività e dei danni causati a terzi che ha come massimali:

- 3.000.000 euro per singolo sinistro;
- 6.000.000 euro per annualità.

## **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 Soggetto 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 Soggetto), date di revoca e di sospensione del certificato}. In particolare, i dati personali vengono trattati da InfoCert in conformità a quanto indicato nel Codice dell'Amministrazione Digitale, nel Decreto Legislativo 30 giugno 2003, n. 196 [4], integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n. 205).

### **9.4.1 Programma sulla privacy**

InfoCert adotta un set di policy tramite le quali implementa e integra la protezione dei

dati personali all'interno del suo Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001, condividendo con quest'ultimo sistema il processo di miglioramento continuo.

#### **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, certificato (se richiesto dal Soggetto), date di revoca e di sospensione del certificato, non sono considerati dati personali.

#### **9.4.4 Titolare del trattamento**

InfoCert S.p.A.

Piazza Sallustion n. 9

00147 Roma

richieste.privacy@legalmail.it

#### **9.4.5 Informativa privacy e consenso al trattamento dei dati personali**

L'informativa privacy è disponibile sul sito [www.infocert.it](http://www.infocert.it).

Prima di eseguire ogni trattamento di dati personali, qualora necessario, InfoCert 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 InfoCert. Tutti i diritti sono riservati.

## **9.6 Rappresentanza e garanzie**

Si rimanda alla contrattualistica stipulata tra CA, RA, Richiedenti e Soggetti per il dettaglio delle garanzie e responsabilità in carico a ciascun soggetto.

## **9.7 Limitazione di garanzia**

Si rimanda alla contrattualistica che regola il servizio per questo aspetto.

## **9.8 Limitazione di responsabilità**

Si rimanda alla contrattualistica che regola il servizio per questo aspetto.

## **9.9 Indennizzi**

Si rimanda alla contrattualistica che regola il servizio per questo aspetto.

## **9.10 Termine e risoluzione**

### **9.10.1 Termine**

Al termine del rapporto tra CA e Soggetto, 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 1.5.2.

## 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

<b>Versione/Release n°:</b>	<b>1.7</b>
<b>Data Versione/Release:</b>	15/05/2024
<b>Descrizione modifiche:</b>	<p>§§ 1.2, 4.1.1: Precisazione con aggiunta sito istituzionale</p> <p>§ 1.3.1: Revisione dati societari</p> <p>§ 1.3.2.1: Precisazioni</p> <p>§§ 1.5.1, 4.9.3: Eliminazione fax dai contatti e revisione contatti</p> <p>§§ 1.5.2, 9.10.7: Aggiornamento denominazioni aree aziendali</p> <p>§ 1.6.1 e 1.6.2: Aggiunta definizione di Cliente, armonizzazione definizioni e acronimi</p> <p>§§ 2.2.3, 2.3.1, 2.3.2: precisazione sull'indirizzo di pubblicazione</p> <p>§ 5.1.1: Revisione descrizione</p> <p>§ 5.1.3: Aggiornamento certificazione del sito</p> <p>§ 5.1.7 e 5.1.8: Revisione descrizione</p> <p>§ 6.2.1: Revisione descrizione</p> <p>§ 6.3.1 Aggiornamento durata del certificato</p>

	<p>§ 8.3: Revisione descrizione</p> <p>§§ 6.1.5, Appendice A: Revisione e modifiche per nuova root CA</p> <p>Revisione generale con correzioni ortografiche e grammaticali e precisazioni</p>
<b>Motivazioni:</b>	<p>Revisione periodica documento</p> <p>Nuova root CA</p>

<b>Versione/Release n°:</b>	<b>1.6</b>
<b>Data Versione/Release:</b>	12/05/2023
<b>Descrizione modifiche:</b>	<p>Modifica logo InfoCert</p> <p>§§ 5.1.1, 5.1.3, 5.1.5 Revisione aspetti di facility</p> <p>§§ 6.1.5, 7.1.3 Revisione algoritmi e chiavi</p> <p>§ Appendice A Aggiornamento formato CRL e OCSP</p>
<b>Motivazioni:</b>	<p>Revisione periodica documento</p> <p>Rebranding</p>

<b>Versione/Release n°:</b>	<b>1.5</b>
<b>Data Versione/Release:</b>	20/05/2022
<b>Descrizione modifiche:</b>	<p>Correzione refusi</p> <p>Formattazione per documento accessibile</p>
<b>Motivazioni:</b>	Revisione periodica documento

<b>Versione/Release n°:</b>	<b>1.4</b>
<b>Data Versione/Release:</b>	24/03/2022
<b>Descrizione modifiche:</b>	aggiunta nuove modalità di identificazione § 3.2.3.4 e 3.2.3.6

<b>Motivazioni:</b>	nuove esigenze di processo
---------------------	----------------------------

<b>Versione/Release n°:</b>	<b>1.3</b>
<b>Data Versione/Release:</b>	08/06/2021
<b>Descrizione modifiche:</b>	<p>correzione refusi,                      revisione e aggiunta policy § 1.2,                      aggiornamento ragione sociale del gruppo § 1.3.1,                      aggiornamento contatti § 1.5.2,                      revisione descrizione § 4.3.1.2,                      aggiunta limite d'uso per finalità di test § 4.5.3,                      aggiornamento tecnologico e riferimenti ai servizi ospitati su cloud AWS § 5.1.1,                      aggiornamento tecnologico § 5.1.6                      aggiornamento descrizione §§ 2.2.3, 5.3.5, 6.1.7                      aggiunta nuova root CA § Appendice A.</p>
<b>Motivazioni:</b>	revisione periodica del documento

<b>Versione/Release n°:</b>	<b>1.2</b>
<b>Data Versione/Release:</b>	25/07/2019
<b>Descrizione modifiche:</b>	<p>correzione refusi,                      modifica logo aziendale,                      aggiornamento normativa sull'antiriciclaggio § 3.23.2,                      aggiornamento normativa privacy § 9.4.</p>
<b>Motivazioni:</b>	revisione del documento per mutato contesto normativo e di business e correzione di refusi

<b>Versione/Release n°:</b>	<b>1.1</b>
<b>Data Versione/Release:</b>	12/07/2017
<b>Descrizione modifiche:</b>	<p>§ 1.3.1.1 semplificazione modalità di nomina dell'IR;</p> <p>§ 1.3.3 correzione refusi</p> <p>§ 1.4.2 correzione refusi;</p> <p>§ 1.6 allineamento definizioni;</p> <p>§ 2.2.1 correzione refusi</p> <p>§ 2.2.2 definizione della non possibilità di pubblicare i certificati;</p> <p>§ 3.2. e § 3.2.3.2 eliminazione del riferimento al D.Lgs 231/2007 per l'Italia, in quanto pleonastici;</p> <p>§ 3.2.1 riscrittura del paragrafo;</p> <p>§ 3.2.3.4 riscrittura del paragrafo senza alterarne il significato; § 3.4.1 correzione refuso;</p> <p>§ 4.1.1 modifica sito web;</p> <p>§ 4.1.2 sostituzione di "iscrizione" con "registrazione";</p> <p>§ 4.3.3.2 modifica procedura di attivazione del dispositivo di firma remota;</p> <p>§ 4.4.2 definizione della non possibilità di pubblicare i certificati; § 4.5.1 correzione refusi;</p> <p>§ 4.9.3.2 semplificazione delle modalità di richiesta di revoca;</p> <p>§ 4.9.6 correzione refuso in struttura del documento;</p> <p>§ 4.9.10, § 4.9.11, § 4.9.12 correzione refusi in struttura del documento;</p> <p>§ 4.10.1 riscrittura paragrafo; § 5.6 riscrittura paragrafo;</p> <p>§ 6.1 inserimento riferimento a CSP ICERT-INDI-TSA;</p> <p>§ 7.3 riscrittura paragrafo; § 8 e § 8.5 correzione refusi;</p> <p>§ 9.1.1 e § 9.1.4 e § 9.1.5 modifica sito web;</p> <p>§ 9.1.2 correzione refuso;</p>

	§ 9.12 correzione refuso; § 9.12.3 semplificazione modalità di reperimento del Manuale Operativo; Appendice A – correzione vari refusi
<b>Motivazioni:</b>	revisione del documento per mutato contesto di business e correzione di refusi

<b>Versione/Release n°:</b>	<b>1.0</b>
<b>Data Versione/Release:</b>	12/12/2016
<b>Descrizione modifiche:</b>	prima emissione
<b>Motivazioni:</b>	prima emissione del documento

### 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 Sicurezza, il Responsabile della Privacy, il Responsabile Legale, il Responsabile Regulatory e approvate dalla Direzione Aziendale.

### 9.12.3 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato in formato elettronico nella sezione dedicata alla documentazione del sito web di InfoCert ([www.infocert.it](http://www.infocert.it)).

### 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**

Si rimanda alla contrattualistica che regola il servizio per il dettaglio sul 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] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy – e 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) e ss.mm.ii
- [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.25 maggio 2017, n. 90 di “Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività' criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006”, che riscrive integralmente, fra gli altri, il decreto legislativo n. 231/2007 in tema di contrasto al riciclaggio e al finanziamento del terrorismo, in attuazione della direttiva (UE) 2015/849 (c.d. IV Direttiva Antiriciclaggio).e ss.mm.ii
- [7] Decreto Legislativo 6 settembre 2005, n.206 e ss.mm.ii - Codice del Consumo

[8] non utilizzato

[9] Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determinazioni successive.

Si applicano inoltre 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 , salvo accordi contrattuali diversi, sono:

<b>Servizio</b>	<b>Orario</b>
<b>Accesso all'archivio pubblico dei certificati (comprende i certificati e le CRL).</b>	Dalle 0:00 alle 24:00 7 giorni su 7
<b>Revoca e sospensione dei certificati.</b>	Dalle 0:00 alle 24:00 7 giorni su 7
<b>Altre attività: registrazione, generazione, pubblicazione, rinnovo<sup>5</sup>.</b>	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi Dalle 9:00 alle 13:00 il sabato
<b>Richiesta e/o verifica di marca temporale.</b>	24hx7gg (disponibilità minima 95%)

<sup>5</sup> L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono scegliere diversi orari di sportello. In ogni caso InfoCert garantisce l'erogazione del proprio servizio negli orari sopra riportati.

# APPENDICE A

## Certificato di ROOT: InfoCert Advanced Electronic Signature CA 3

```
0 1848: SEQUENCE {
4 1312: 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
   : }
31 154: SEQUENCE {
34 11: SET {
36 9: SEQUENCE {
38 3: OBJECT IDENTIFIER countryName (2 5 4 6)
43 2: PrintableString 'IT'
   : }
   : }
47 24: SET {
49 22: SEQUENCE {
51 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
56 15: UTF8String 'InfoCert S.p.A.'
   : }
   : }
```

```
73 31:  SET {
75 29:  SEQUENCE {
77 3:   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
82 22:  UTF8String 'Trust Service Provider'
      :   }
      :   }
106 26: SET {
108 24: SEQUENCE {
110 3:  OBJECT IDENTIFIER '2 5 4 97'
115 17: UTF8String 'VATIT-07945211006'
      :   }
      :   }
134 52: SET {
136 50: SEQUENCE {
138 3:  OBJECT IDENTIFIER commonName (2 5 4 3)
143 43: UTF8String
      :   'InfoCert Advanced Electronic Signature CA 3'
      :   }
      :   }
      :   }
188 30: SEQUENCE {
190 13: UTCTime 12/12/2016 16:45:37 GMT
205 13: UTCTime 12/12/2032 17:45:37 GMT
      :   }
220 154: SEQUENCE {
223 11: SET {
225 9:  SEQUENCE {
227 3:  OBJECT IDENTIFIER countryName (2 5 4 6)
232 2:  PrintableString 'IT'
```

```
      :      }
      :      }
236 24:  SET {
238 22:  SEQUENCE {
240 3:   OBJECT IDENTIFIER organizationName (2 5 4 10)
245 15:  UTF8String 'InfoCert S.p.A.'
      :      }
      :      }
262 31:  SET {
264 29:  SEQUENCE {
266 3:   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
271 22:  UTF8String 'Trust Service Provider'
      :      }
      :      }
295 26:  SET {
297 24:  SEQUENCE {
299 3:   OBJECT IDENTIFIER '2 5 4 97'
304 17:  UTF8String 'VATIT-07945211006'
      :      }
      :      }
323 52:  SET {
325 50:  SEQUENCE {
327 3:   OBJECT IDENTIFIER commonName (2 5 4 3)
332 43:  UTF8String
      :      'InfoCert Advanced Electronic Signature CA 3'
      :      }
      :      }
      :      }
377 546: SEQUENCE {
```

```

381 13: SEQUENCE {
383 9:  OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
394 0:  NULL
      :  }
396 527: BIT STRING, encapsulates {
401 522: SEQUENCE {
405 513: INTEGER
      :  00 D9 F0 76 FE E9 14 07 07 DD 31 2B 48 E1 1A 93
      :  DC 42 43 C1 ED 3D 96 36 DF 49 F6 A7 E9 58 BB A0
      :  34 E2 8D 77 77 1F 73 CD 17 37 28 50 F6 4D 18 C9
      :  0E 78 81 DA 15 77 02 8D 1F DA C5 1F 28 E9 5D B2
      :  3F 07 3A 8F 4D 00 DB 76 40 6A CA D3 87 BA AA 43
      :  7C AE C5 E6 2B 60 B8 7E 65 64 F3 F1 06 B2 94 95
      :  6F C5 1E 3E 39 39 41 17 44 A9 87 E2 D6 EB 08 35
      :  5E 2E 7E 3B E8 6A E0 6E DB 57 F6 32 34 76 36 55
      :  [ Another 385 bytes skipped ]
922 3:  INTEGER 65537
      :  }
      :  }
      :  }
927 389: [3] {
931 385: SEQUENCE {
935 15: SEQUENCE {
937 3:  OBJECT IDENTIFIER basicConstraints (2 5 29 19)
942 1:  BOOLEAN TRUE
945 5:  OCTET STRING, encapsulates {
947 3:  SEQUENCE {
949 1:  BOOLEAN TRUE
      :  }

```

```

:      }
:      }
952 88: SEQUENCE {
954 3:  OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
959 81: OCTET STRING, encapsulates {
961 79: SEQUENCE {
963 77: SEQUENCE {
965 4:  OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
971 69: SEQUENCE {
973 67: SEQUENCE {
975 8:  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
985 55: IA5String
:      'http://www.firma.infocert.it/documentazione/manu'
:      'ali.php'
:      }
:      }
:      }
:      }
:      }
:      }
:      }
1042 228: SEQUENCE {
1045 3:  OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1050 220: OCTET STRING, encapsulates {
1053 217: SEQUENCE {
1056 214: SEQUENCE {
1059 211: [0] {
1062 208: [0] {
1065 39:  [6] 'http://crl.infocert.it/ca3/ades/ARL.crl'
1106 164: [6]

```

```

:      'ldap://ldap.infocert.it/cn%3DInfoCert%20Advanced'
:      '%20Electronic%20Signature%20CA%203,ou%3DTrust%20'
:      'Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?aut'
:      'horityRevocationList'
:      }
:      }
:      }
:      }
:      }
:      }
:      }
:      }
:      }
1273 14: SEQUENCE {
1275 3:   OBJECT IDENTIFIER keyUsage (2 5 29 15)
1280 1:   BOOLEAN TRUE
1283 4:   OCTET STRING, encapsulates {
1285 2:     BIT STRING 1 unused bit
:       '1100000'B
:       }
:       }
1289 29: SEQUENCE {
1291 3:   OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1296 22:  OCTET STRING, encapsulates {
1298 20:   OCTET STRING
:       2E B8 32 31 EF 4F 33 13 70 04 23 1D BE 8B 48 9D
:       B1 5F E0 51
:       }
:       }
:       }
:       }
:       }
:       }
:       }
:       }
:       }

```

```
1320 13: SEQUENCE {
1322 9:  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1333 0:  NULL
      :  }
1335 513: BIT STRING
      :  42 9D E2 BD 74 54 70 30 5F 57 6E 3C 6A 5D 27 94
      :  07 85 3E 80 D5 DC DE 56 73 91 34 A2 59 3D 5C 23
      :  AC 3B 55 52 E3 1F BC 9A CE 44 FA 72 CE 7A 50 46
      :  FB 9E AB 21 B5 57 B7 89 7E 1B 2B 66 E9 5D F4 AE
      :  5A 05 EC E3 D3 11 4B D5 39 A7 B3 1B 8C 78 C2 9F
      :  BF A2 BE 32 EA 59 0F 7B DA DC 3F EA 53 EA 36 A0
      :  A6 72 C6 1C 61 C0 A2 F0 B7 2E 9D 61 BE 89 45 B4
      :  F2 C7 3A B1 99 A8 13 BE 68 33 49 35 A0 1A 1B 3A
      :  [ Another 384 bytes skipped ]
      :  }
```

## Certificato di ROOT: InfoCert Advanced Electronic Signature CA 4

```
0 1673: SEQUENCE {
4 1137: 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
      :  }
31 154: SEQUENCE {
34 11:  SET {
36 9:   SEQUENCE {
38 3:   OBJECT IDENTIFIER countryName (2 5 4 6)
43 2:   PrintableString 'IT'
      :   }
      :   }
47 24:  SET {
49 22:  SEQUENCE {
51 3:   OBJECT IDENTIFIER organizationName (2 5 4 10)
56 15:  UTF8String 'InfoCert S.p.A.'
      :   }
      :   }
73 31:  SET {
75 29:  SEQUENCE {
77 3:   OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
82 22:  UTF8String 'Trust Service Provider'
      :   }
      :   }
106 26: SET {
108 24: SEQUENCE {
110 3:  OBJECT IDENTIFIER '2 5 4 97'
115 17: UTF8String 'VATIT-07945211006'
      :   }
      :   }
134 52: SET {
```

```

136 50: SEQUENCE {
138 3: OBJECT IDENTIFIER commonName (2 5 4 3)
143 43: UTF8String
      : 'InfoCert Advanced Electronic Signature CA 4'
      : }
      : }
      : }
188 30: SEQUENCE {
190 13: UTCTime 07/06/2021 08:35:29 GMT
205 13: UTCTime 07/06/2036 09:35:29 GMT
      : }
220 154: SEQUENCE {
223 11: SET {
225 9: SEQUENCE {
227 3: OBJECT IDENTIFIER countryName (2 5 4 6)
232 2: PrintableString 'IT'
      : }
      : }
236 24: SET {
238 22: SEQUENCE {
240 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
245 15: UTF8String 'InfoCert S.p.A.'
      : }
      : }
262 31: SET {
264 29: SEQUENCE {
266 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
271 22: UTF8String 'Trust Service Provider'
      : }

```

```

:   }
295 26: SET {
297 24: SEQUENCE {
299 3: OBJECT IDENTIFIER '2 5 4 97'
304 17: UTF8String 'VATIT-07945211006'
:   }
:   }
323 52: SET {
325 50: SEQUENCE {
327 3: OBJECT IDENTIFIER commonName (2 5 4 3)
332 43: UTF8String
:   'InfoCert Advanced Electronic Signature CA 4'
:   }
:   }
:   }
377 546: SEQUENCE {
381 13: SEQUENCE {
383 9: OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
394 0: NULL
:   }
396 527: BIT STRING, encapsulates {
401 522: SEQUENCE {
405 513: INTEGER
:   00 C3 BB 3C 19 5E B2 5E A6 81 0D 21 31 82 12 32
:   31 D6 D6 BD 78 97 7C 39 CA 15 C0 37 AA 1D 9B ED
:   45 34 02 77 EE 95 8C AE 26 CF 87 E4 82 81 E1 D2
:   34 6A 14 1C 21 B9 EA C9 76 E3 78 4F 79 B4 94 2B
:   40 D8 F8 A7 F5 EA 86 20 58 8F 69 43 75 9D 21 F3
:   4C B9 E2 67 86 B9 1C 11 49 A4 1E A1 4C 59 6D 6F

```



```

:   }
:   }
927 215: [3] {
930 212: SEQUENCE {
933 15: SEQUENCE {
935 3: OBJECT IDENTIFIER basicConstraints (2 5 29 19)
940 1: BOOLEAN TRUE
943 5: OCTET STRING, encapsulates {
945 3: SEQUENCE {
947 1: BOOLEAN TRUE
:   }
:   }
:   }
950 88: SEQUENCE {
952 3: OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
957 81: OCTET STRING, encapsulates {
959 79: SEQUENCE {
961 77: SEQUENCE {
963 4: OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
969 69: SEQUENCE {
971 67: SEQUENCE {
973 8: OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
983 55: IA5String
: 'http://www.firma.infocert.it/documentazione/manu'
: 'ali.php'
:   }
:   }
:   }
:   }

```

```

:      }
:      }
1040 56: SEQUENCE {
1042 3:  OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1047 49: OCTET STRING, encapsulates {
1049 47: SEQUENCE {
1051 45: SEQUENCE {
1053 43: [0] {
1055 41: [0] {
1057 39: [6] 'http://crl.ca4.infocert.it/ades/ARL.crl'
:      }
:      }
:      }
:      }
:      }
:      }
1098 14: SEQUENCE {
1100 3:  OBJECT IDENTIFIER keyUsage (2 5 29 15)
1105 1: BOOLEAN TRUE
1108 4: OCTET STRING, encapsulates {
1110 2: BIT STRING 1 unused bit
:      '1100000'B
:      }
:      }
1114 29: SEQUENCE {
1116 3:  OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1121 22: OCTET STRING, encapsulates {
1123 20: OCTET STRING
:      84 B0 C8 E9 41 16 7C 8F B2 96 8E 70 2D 13 DD 14

```

```
      :      58 96 87 A2
      :      }
      :      }
      :      }
      :      }
      :      }
      :      }
1145 13: SEQUENCE {
1147  9:  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1158  0:  NULL
      :  }
1160 513: BIT STRING
      :  09 B7 20 4A 06 28 B6 50 70 6E 46 63 36 0E A1 BF
      :  64 2C 60 F3 A9 23 2A A1 D3 DA 86 E7 0D 4F 99 CD
      :  E0 8B 1E 76 F3 7C 63 DE F0 A8 51 C3 97 B8 17 BA
      :  E2 9D 87 CC A6 24 BE C1 D2 6C D7 3A 76 36 D4 5B
      :  0F 71 19 DC 61 53 9F F4 0B EE B7 8A 6F B3 AE 2B
      :  4C 4B 11 92 2F ED B9 0F 25 4D A1 30 1F 5E EF 7F
      :  05 43 5F 56 5D 16 2A E4 F8 9C D6 1E DC CB A8 9A
      :  71 37 FF FA 47 BB 3B 98 50 4D 7C A0 F1 A1 38 DB
      :  7D C4 B9 50 E6 46 2E 66 09 2B 9B C4 35 C4 6B A3
      :  2D 86 24 9B 29 28 A8 52 3B 09 92 99 F2 4E 9C 05
      :  BE 33 D7 11 6C CB 86 3D 52 97 40 C5 FA 6C E2 13
      :  DD B3 1B 30 E4 D0 4F 08 AF C0 B9 27 4D A8 05 7D
      :  BE 73 AE 97 F5 BA CB D5 A7 6A DB 19 00 C4 F0 E7
      :  42 51 F3 EB 4A 94 F5 78 2A B1 F1 29 8A D1 71 46
      :  D2 90 B0 A8 A0 39 37 4E 74 C6 95 05 41 56 BF 22
      :  C0 13 96 05 F5 BA 50 60 93 84 44 A0 D2 91 77 51
      :  52 B9 25 32 A3 E9 13 76 5E 5A BF 08 76 C0 30 3F
      :  8B 1B D1 0B 04 5C 0D 4F 2B 1F FC 3B D4 F4 DF FE
```

: 6A 40 30 1B 1D 4C 73 DA 7F 46 B5 58 CE C1 14 21  
: 94 42 82 39 01 6A D2 BB 04 60 D5 95 15 96 DA 4F  
: 3C DA 7C A5 66 19 0E E6 DC C9 70 AE B0 F7 D5 7E  
: 60 92 90 26 FD 23 5E 0C F1 98 DD 92 8B 82 89 F5  
: 4B C1 30 0C BF 10 F5 A2 81 E2 84 2E 85 8E 13 CE  
: 31 D9 10 74 34 48 86 95 10 8C 2E F3 31 40 77 B5  
: 0D A4 01 2A 58 AA A2 90 15 06 07 A6 B0 7E 8F 96  
: 57 62 15 84 89 FB 73 27 F2 78 CD 60 C8 52 51 ED  
: D9 15 BA 2C 50 E0 F2 C6 9F 14 0A 33 ED 5D 98 5C  
: C1 D9 11 49 DB 64 1E 62 B0 F1 B9 CC 33 93 BE 49  
: 9E 71 E5 CA B4 3A ED 67 9A 92 FD 73 48 83 40 A4  
: B3 A7 0A 1F 88 08 0A C8 21 F4 FD 39 34 28 90 F8  
: D8 25 71 FC 75 12 A0 E9 FD 72 2D E1 EA 1C 02 7B  
: 55 EC 0B 5F 7C 5B BA D6 E7 BA 1B AB AE 69 80 05  
: }

## Certificato di ROOT: InfoCert Advanced Electronic Signature EC CA 4

0 853: SEQUENCE {  
4 731: SEQUENCE {  
8 3: [0] {  
10 1: INTEGER 2  
: }  
13 20: INTEGER 75 1C F9 49 E4 48 C4 C7 77 34 5A 6F CB 7D 5E 55 3D 5B AE 2E  
35 10: SEQUENCE {  
37 8: OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)  
: }  
47 157: SEQUENCE {

```
50 11: SET {
52 9: SEQUENCE {
54 3: OBJECT IDENTIFIER countryName (2 5 4 6)
59 2: PrintableString 'IT'
: }
: }
63 24: SET {
65 22: SEQUENCE {
67 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
72 15: UTF8String 'InfoCert S.p.A.'
: }
: }
89 31: SET {
91 29: SEQUENCE {
93 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
98 22: UTF8String 'Trust Service Provider'
: }
: }
122 26: SET {
124 24: SEQUENCE {
126 3: OBJECT IDENTIFIER '2 5 4 97'
131 17: UTF8String 'VATIT-07945211006'
: }
: }
150 55: SET {
152 53: SEQUENCE {
154 3: OBJECT IDENTIFIER commonName (2 5 4 3)
159 46: UTF8String
: 'InfoCert Advanced Electronic Signature EC CA 4'
```

```

    :   }
    :   }
    :   }
207 30: SEQUENCE {
209 13:   UTCTime 15/05/2024 14:22:49 GMT
224 13:   UTCTime 15/05/2036 14:22:49 GMT
    :   }
239 157: SEQUENCE {
242 11:   SET {
244 9:    SEQUENCE {
246 3:    OBJECT IDENTIFIER countryName (2 5 4 6)
251 2:    PrintableString 'IT'
    :    }
    :    }
255 24:   SET {
257 22:   SEQUENCE {
259 3:    OBJECT IDENTIFIER organizationName (2 5 4 10)
264 15:   UTF8String 'InfoCert S.p.A.'
    :    }
    :    }
281 31:   SET {
283 29:   SEQUENCE {
285 3:    OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
290 22:   UTF8String 'Trust Service Provider'
    :    }
    :    }
314 26:   SET {
316 24:   SEQUENCE {
318 3:    OBJECT IDENTIFIER '2 5 4 97'
```

```

323 17:    UTF8String 'VATIT-07945211006'
      :    }
      :    }
342 55:    SET {
344 53:    SEQUENCE {
346 3:     OBJECT IDENTIFIER commonName (2 5 4 3)
351 46:    UTF8String
      :    'InfoCert Advanced Electronic Signature EC CA 4'
      :    }
      :    }
      :    }
399 118:   SEQUENCE {
401 16:    SEQUENCE {
403 7:     OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
412 5:     OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
      :    }
419 98:    BIT STRING
      :    04 52 48 48 57 3B 2D 80 C5 21 D0 73 3D 52 A2 45
      :    3B 8E 18 1F EE BB AE 08 82 B8 E2 51 4F 04 98 BE
      :    FB 47 69 10 8B F3 5E C6 83 B1 F3 AF D1 63 9E 3E
      :    4D 64 CF E1 D4 09 89 A8 41 EF 06 C3 C2 9B B9 16
      :    11 02 F2 D0 E6 1E A6 2B 33 12 20 04 9E 79 38 C6
      :    0F D8 34 41 C4 C7 9F 8E 95 51 D4 E3 7B 29 45 8D
      :    C9
      :    }
519 217:   [3] {
522 214:   SEQUENCE {
525 15:    SEQUENCE {
527 3:     OBJECT IDENTIFIER basicConstraints (2 5 29 19)

```

```

532 1:    BOOLEAN TRUE
535 5:    OCTET STRING, encapsulates {
537 3:    SEQUENCE {
539 1:    BOOLEAN TRUE
      :    }
      :    }
      :    }
542 88:   SEQUENCE {
544 3:    OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
549 81:   OCTET STRING, encapsulates {
551 79:   SEQUENCE {
553 77:   SEQUENCE {
555 4:    OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
561 69:   SEQUENCE {
563 67:   SEQUENCE {
565 8:    OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
575 55:   IA5String
      :    'http://www.firma.infocert.it/documentazione/manu'
      :    'ali.php'
      :    }
      :    }
      :    }
      :    }
      :    }
      :    }
      :    }
632 58:   SEQUENCE {
634 3:    OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
639 51:   OCTET STRING, encapsulates {
641 49:   SEQUENCE {

```

```
643 47:      SEQUENCE {
645 45:      [0] {
647 43:      [0] {
649 41:      [6]
      :      'http://crl.ca4.infocert.it/adesec/ARL.crl'
      :      }
      :      }
      :      }
      :      }
      :      }
      :      }
      :      }
692 14:      SEQUENCE {
694 3:      OBJECT IDENTIFIER keyUsage (2 5 29 15)
699 1:      BOOLEAN TRUE
702 4:      OCTET STRING, encapsulates {
704 2:      BIT STRING 1 unused bit
      :      '1100000'B
      :      }
      :      }
708 29:      SEQUENCE {
710 3:      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
715 22:      OCTET STRING, encapsulates {
717 20:      OCTET STRING
      :      80 7D 38 65 A1 43 A6 49 9C FB F2 FE 6D 55 28 B9
      :      E5 47 A2 B4
      :      }
      :      }
      :      }
      :      }
```

```

: }
739 10: SEQUENCE {
741 8:  OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
: }
751 104: BIT STRING, encapsulates {
754 101:  SEQUENCE {
756 48:    INTEGER
:      04 F7 CF B8 C9 24 75 82 3B 7F 35 95 38 B2 B4 4D
:      45 1F AA 96 7F AA 36 E5 27 FB CF 3B 34 00 BF CD
:      DB FF B1 99 F5 30 59 AF 09 BC 84 2B 80 69 CE F5
806 49:    INTEGER
:      00 BC 03 85 69 8A 40 77 A7 D1 09 42 13 CB 84 3D
:      29 1D 24 FB 4A E6 96 8C 12 BF 8D AF DA 90 9C F5
:      B7 B1 36 E9 2D D5 2C 2B 5F CC 16 C0 CB C3 AB 23
:      B1
:    }
: }
: }
: }

```

## Formato delle CRL e OCSP

Estensione	Valore
Issuer Algorithm                      Signature	In base alla chiave del certificato di root CA, scelto tra  sha256WithRSAEncryption [iso(1) member-body(2) us(840)                      rsadsi(113549)                      pkcs(1)                      pkcs-1(1) sha256WithRSAEncryption(11)]  ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi- x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-

	with-SHA256(2)]  ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]  ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer Distinguished Name	InfoCert
thisUpdate	Data in formato UTC
nextUpdate	Data della prossima CRL In format
Revoked Certificates List	Lista dei certificati revocati, con numero di serie e data di revoca/sospensione
Issuer's Signature	Firma della CA

## Valori ed estensioni per CRL e OCSP

Le CRL hanno le seguenti estensioni

Extension	Value
<b>Authority Key Identifier</b>	Il valore dell'impronta 160-bit SHA-1 di issuerPublicKey
<b>CRL number</b>	Il numero univoco della CRL assegnato dalla CA
<b>ExpiredCertsOnCRL</b>	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
<b>Issuing Distribution Point</b>	Identifica il punto di distribuzione delle CRL e lo scopo: indica se la CRL è generata solo per certificati di CA, o del soggetto (end-entity)
<b>Invalidity Date</b>	Data in formato UTC che indica la data da cui si ritiene che il certificato sia invalido

La richiesta OCSP contiene i seguenti campi:

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] 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 della risposta OCSP.
Produced at	Data in formato GeneralizedTime di quando è stata generate la risposta
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	La data in cui lo stato del certificato potrebbe essere aggiornato
Issuer Signature Algorithm	In base alla chiave del certificato di OCSP Responder, scelto tra

	<p>sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]</p> <p>ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]</p> <p>ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]</p> <p>ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]</p>
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.

La risposta 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. È contenuto in una requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in

	una responseExtensions.
--	-------------------------