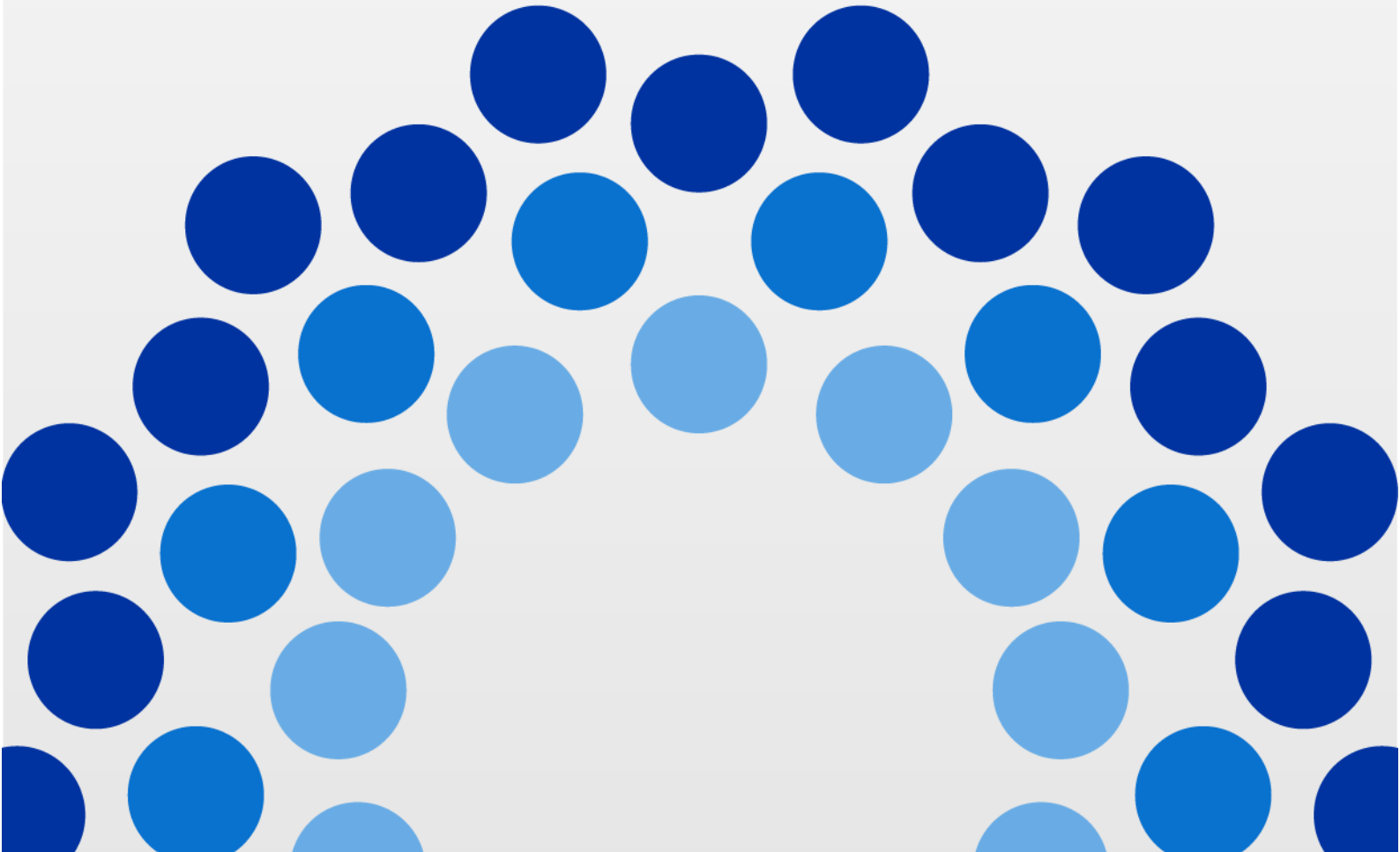
Manuale Operativo

Certificate Policy e Certificate Practice Statement

Certificati qualificati

CODICE DOCUMENTO	IC-MO-TSP
VERSIONE	5
DATA	28/12/2023



STORIA DELLE MODIFICHE

Versione	Data	Modifiche
1	10/02/2020	Prima versione del documento
2	28/04/2021	Intero documento: correzioni refusi Introduzione § 3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati a seguito di revoca Integrazioni al § 4.2.1.1: indicazione univocità del contatto email associato al Titolare § 4.9.13 sospensione cautelativa da parte della CA
3	27/07/2021	§3.2.3.3 Aggiunti ulteriori mezzi di identificazione elettronica modalità 3 – AuthenticationID §4.5.3 Aggiunto limite d'uso per emissione con SPID e aggiornata descrizione limite di valore Rivisti i §9.1.5 Politiche per il rimborso, §9.10.2 Risoluzione, §9.14 Foro competente
4	16/12/2022	Intero documento: revisione annuale § 4.3.1.4 Emissione del certificato con finalità di test §3.2.3.1 e §9.15 Inserito riferimento ad "Allegato al Manuale Operativo / Certificate Policy e Certificate Practice Statement Certificati qualificati - Documenti di riconoscimento consentiti" Adeguamento normativo
5	28/12/2023	Intero documento: revisione annuale §1.6.1 Aggiunto riferimento a standard ETSI 319 411-1 Aggiunto riferimento a Determinazione AgID 147/2019 § 3.1.1 Deroga a RFC 5280 per la lunghezza di alcuni campi del subjectDN §4.9 Inserita informazioni sulla conservazione dello stato di revoca a seguito della scadenza del certificate di root. §4.9.3 Integrati riferimenti per certificati short-term § 5.1.6 Aggiornamento tecnologico dei supporti di Memorizzazione §5.7.3 Precisazioni su compromissioni delle chiavi §5.8 Inserita informazioni sulla conservazione dello stato di revoca in caso di cessazionne della CA. §6.1.7 Modifica paragrafo con specifiche su utilizzo della chiave di CA (§6.1.7.1) e utilizzo della chiave del Titolare (§6.1.7.2) §9.17 Aggiornamento orari di erogazione servizi

SOMMARIO

Manuale Operativo....0
1 INTRODUZIONE....11
1.1 Quadro generale....11
1.2 Nome ed identificativo del documento....11
1.3 Partecipanti e responsabilità....13
1.3.1 Certification Authority – Autorità di Certificazione....13
1.3.2 Registration Authority – Ufficio di Registrazione (RA)....13
1.3.3 Soggetto....14
1.3.4 Utente....14
1.3.5 Richiedente....14
1.3.6 Autorità....15
1.4 Uso del certificato....15
1.4.1 Usi consentiti....15
1.4.2 Usi non consentiti....15
1.5 Amministrazione del Manuale Operativo....16
1.5.1 Contatti....16
1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo....16
1.5.3 Procedure di approvazione....16
1.6 Definizioni e acronimi....16
1.6.1 Definizioni....16
1.6.2 Acronimi e abbreviazioni....21
2 PUBBLICAZIONE E ARCHIVIAZIONE....23
2.1 Archiviazione....23
2.2 Pubblicazione delle informazioni sulla certificazione....23
2.2.1 Pubblicazione del manuale operativo....23
2.2.2 Pubblicazione dei certificati....23
2.2.3 Pubblicazione delle liste di revoca e sospensione....23
2.3 Periodo o frequenza di pubblicazione....24

2.3.1 Frequenza di pubblicazione del manuale operativo 24
2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione 24
2.4 Controllo degli accessi agli archivi pubblici 24
3 IDENTIFICAZIONE E AUTENTICAZIONE 25
3.1 Denominazione 25
3.1.1 Tipi di nomi 25
3.1.2 Necessità che il nome abbia un significato 25
3.1.3 Anonimato e pseudonimia dei richiedenti 25
3.1.4 Regole di interpretazione dei tipi di nomi 25
3.1.5 Univocità dei nomi 26
3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati 26
3.2 Convalida iniziale dell'identità 26
3.2.1 Metodo per dimostrare il possesso della chiave privata 26
3.2.2 Identificazione dell'identità delle organizzazioni 27
3.2.3 Identificazione della persona fisica 27
3.2.4 Informazioni del Soggetto o del Richiedente non verificate 29
3.2.5 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
3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati a seguito di revoca 31
3.4 Identificazione e autenticazione per le richieste di revoca o sospensione 31
3.4.1 Richiesta da parte del Soggetto 31
3.4.2 Richiesta da parte del Richiedente 31
4 OPERATIVITÀ 33
4.1 Richiesta del certificato 33
4.1.1 Chi può richiedere un certificato 33
4.1.2 Processo di registrazione e responsabilità 33
4.2 Elaborazione della richiesta 33
4.2.1 Informazioni che il Soggetto deve fornire 34
4.2.2 Approvazione o rifiuto della richiesta del certificato 35
4.2.3 Tempo massimo per l'elaborazione della richiesta del certificato 35

4.3 Emissione del certificato 36
4.3.1 Azioni della CA durante l'emissione del certificato 36
4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato 37
4.3.3 Attivazione 37
4.4 Accettazione del certificato 38
4.4.1 Comportamenti concludenti di accettazione del certificato 38
4.4.2 Pubblicazione del certificato da parte della Certification Authority 38
4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato 38
4.5 Uso della coppia di chiavi e del certificato 38
4.5.1 Uso della chiave privata e del certificato da parte del Soggetto 38
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 39
4.6 Rinnovo del certificato 39
4.6.1 Motivi per il rinnovo 39
4.6.2 Chi può richiedere il rinnovo 40
4.6.3 Elaborazione della richiesta di rinnovo del certificato 40
4.7 Riemissione del certificato 40
4.8 Modifica del certificato 40
4.9 Revoca e sospensione del certificato 40
4.9.1 Motivi per la revoca 40
4.9.2 Chi può richiedere la revoca 41
4.9.3 Procedure per richiedere la revoca 41
4.9.4 Periodo di grazia della richiesta di revoca 42
4.9.5 Tempo massimo di elaborazione della richiesta di revoca 42
4.9.6 Requisiti per la verifica della revoca 43
4.9.7 Frequenza di pubblicazione della CRL 43
4.9.8 Latenza massima della CRL 43
4.9.9 Servizi online di verifica dello stato di revoca del certificato 43
4.9.10 Requisiti servizi online di verifica 43
4.9.11 Altre forme di revoca 43
4.9.12 Requisiti specifici rekey in caso di compromissione 44

4.9.13 Motivi per la sospensione 44
4.9.14 Chi può richiedere la sospensione 44
4.9.15 Procedure per richiedere la sospensione 44
4.9.16 Limiti al periodo di sospensione 45
4.10 Servizi riguardanti lo stato del certificato 46
4.10.1 Caratteristiche operative 46
4.10.2 Disponibilità del servizio 46
4.10.3 Caratteristiche opzionali 46
4.11 Disdetta dai servizi della CA 46
4.12 Deposito presso terzi e recovery della chiave 46
5 MISURE DI SICUREZZA E CONTROLLI 47
5.1 Sicurezza fisica 47
5.1.1 Posizione e costruzione della struttura 47
5.1.2 Accesso fisico 48
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 fornita al personale 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 54
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
6 CONTROLLI DI SICUREZZA TECNOLOGICA 56
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 56
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 57
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 58
6.2.6 Trasferimento della chiave privata da un modulo o su un modulo crittografico 58
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 59
6.3.2 Periodo di validità del certificato e della coppia di chiavi 59
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
6.8 Sistema di validazione temporale 61
7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP 62
7.1 Formato del certificato 62
7.1.1 Numero di versione 62
7.1.2 Estensioni del certificato 62
7.1.3 OID dell'algoritmo di firma 62
7.1.4 Forme di nomi 62
7.1.5 Vincoli ai nomi 62
7.1.6 OID del certificato 62
7.2 Formato della CRL 63

7.2.1 Numero di versione 63
7.2.2 Estensioni della CRL 63
7.3 Formato dell'OCSP 63
7.3.1 Numero di versione 63
7.3.2 Estensioni dell'OCSP 63
8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ 64
8.1 Frequenza o circostanze per la valutazione di conformità 64
8.2 Identità e qualifiche di chi effettua il controllo 64
8.3 Rapporti tra InfoCamere e CAB 65
8.4 Aspetti oggetto di valutazione 65
8.5 Azioni in caso di non conformità 65
9 ALTRI ASPETTI LEGALI E DI BUSINESS 66
9.1 Tariffe 66
9.1.1 Tariffe per il rilascio e il rinnovo dei certificati 66
9.1.2 Tariffe per l'accesso ai certificati 66
9.1.3 Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati 66
9.1.4 Tariffe per altri servizi 66
9.1.5 Politiche per il rimborso 66
9.2 Responsabilità finanziaria 66
9.2.1 Copertura assicurativa 66
9.2.2 Altre attività 67
9.2.3 Garanzia o copertura assicurativa per i soggetti finali 67
9.3 Confidenzialità delle informazioni di business 67
9.3.1 Ambito di applicazione delle informazioni confidenziali 67
9.3.2 Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali 67
9.3.3 Responsabilità di protezione delle informazioni confidenziali 67
9.4 Privacy 67
9.4.1 Programma sulla privacy 68
9.4.2 Dati che sono trattati come personali 68
9.4.3 Dati non considerati come personali 68
9.4.4 Titolare del trattamento dei dati personali 68

9.4.5 Informativa privacy e consenso al trattamento dei dati personali 68
9.4.6 Divulgazione dei dati a seguito di richiesta da parte dell'autorità 68
9.4.7 Altri motivi di divulgazione 68
9.5 Proprietà intellettuale 68
9.6 Rappresentanza e garanzie 69
9.6.1 Certification Authority 69
9.6.2 Registration Authority 69
9.6.3 Titolare 69
9.6.4 Relying Party 70
9.6.5 Altri soggetti 70
9.7 Limitazioni di garanzia 70
9.8 Limitazioni di responsabilità 71
9.9 Indennizzi 71
9.10 Termine e risoluzione 72
9.10.1 Termine 72
9.10.2 Risoluzione 72
9.10.3 Effetti della risoluzione 72
9.11 Canali di comunicazione ufficiali 72
9.12 Revisione del Manuale Operativo 72
9.12.1 Storia delle revisioni 73
9.12.2 Procedure di revisione 74
9.12.3 Periodo e meccanismo di notifica 74
9.12.4 Casi nei quali l'OID deve cambiare 74
9.13 Risoluzione delle controversie 74
9.14 Foro competente 74
9.15 Legge applicabile 75
9.16 Disposizioni varie 75
9.17 Altre disposizioni 75
Appendice A 77
Certificato di root CA 77
Formato delle CRL e OCSP 80

Valori ed estensioni per CRL e OCSP..... 80

Appendice B.....83

Avvertenza 84

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 qualificata 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 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 pubblico è il Manuale Operativo o anche "Certification Practice Statement" del **Prestatore di Servizi Fiduciari InfoCamere** (*Trust Service Provider*) che, tra i servizi fiduciari, fornisce anche servizi di firma elettronica qualificata. Il manuale contiene le politiche e le pratiche seguite nel processo di identificazione e emissione del certificato qualificato, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, e in generale di tutto ciò che rende affidabile un certificato qualificato, in conformità con la vigente normativa in materia di servizi fiduciari, firma elettronica e sigillo qualificati e firma digitale.

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 InfoCamere – Manuale Operativo" ed è caratterizzato dal codice documento: **IC-MO-TSP**. La versione e il livello di rilascio sono identificabili nell'intestazione di 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.

Le Policy OID contraddistinguono ciascun profilo di certificato emesso da InfoCamere.

L'*object identifier* (OID) che identifica InfoCamere è 1.3.76.14

Le policy per certificati qualificati su dispositivo qualificato sono:

Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo qualificato (QSCD)	1.3.76.14.1.1.30 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona fisica per firma automatica remota su dispositivo (QSCD)	1.3.76.14.1.1.41 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo (QSCD)	1.3.76.14.1.1.40 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo qualificato di tipo one-shot	1.3.76.14.1.1.42 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona giuridica su dispositivo (QSCD)	1.3.76.14.1.1.50 conforme alla policy QCP-l-qscd 0.4.0.194112.1.3

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.

Inoltre, tutti i certificati che rispettano le raccomandazioni delle Linee Guida in materia di "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" di cui alla Determinazione n. 147 del 4 giugno 2019 emessa dall'Agenzia per l'Italia Digitale (AgID) che ha confermato il contenuto della sua precedente Determinazione n.121/2019 del 17 maggio 2019, conterranno un ulteriore elemento PolicyIdentifier con valore agIDcert (OID 1.3.76.16.6) nel campo CertificatePolicies (OID 2.5.29.32).[1]

Questo documento è pubblicato in formato elettronico presso il sito Web del Prestatore di Servizi Fiduciari all'indirizzo https://id.infocamere.it/ nella sezione Documentazione.

[1] L'assenza di tale OID può comportare la non adeguatezza di servizi in rete offerti nello specifico contesto italiano. Un esempio, in tal senso, è l'assenza dell'obbligo di indicare nel certificato qualificato per la generazione della firma il codice fiscale del titolare, elemento indispensabile per diverse pubbliche amministrazioni italiane.

1.3 Partecipanti e responsabilità

1.3.1 Certification Authority – Autorità di Certificazione

La **Certification Authority** è il soggetto terzo e fidato che emette i certificati qualificati di firma elettronica qualificata, firmandoli con la propria chiave privata, detta chiave di CA o chiave di root.

InfoCamere è la Certification Authority (**CA**) che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle regole tecniche emanate dall'Autorità di Vigilanza e secondo quanto prescritto dal Regolamento eIDAS [1] e dal Codice dell'Amministrazione Digitale [2].

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

Denominazione sociale	**InfoCamere S.C.p.A.**
Sede legale	Via G.B. Morgagni, 13 – 00161 Roma
Sede operativa	Corso Stati Uniti 14 - 35127 Padova
Rappresentante legale	Tagliavanti Lorenzo
N. di telefono	06-442851
N. Iscrizione Registro Imprese	Codice Fiscale 02313821007
N. partita IVA	02313821007
Sito web	https://www.infocamere.it

1.3.2 Registration Authority – Ufficio di Registrazione (RA)

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

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

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

Le RA sono attivate dalla CA a seguito di un adeguato addestramento del personale impiegato.

Le RA sono inoltre soggette a verifiche periodiche da parte di InfoCamere con lo scopo di accertare il rispetto degli accordi sottoscritti con la CA e delle procedure definite nel presente Manuale.

1.3.2.1 Operatore di Registrazione (ODR / RAO) e Incaricato alla Registrazione (IR)

La RA può nominare, utilizzando apposita modulistica, persone fisiche o giuridiche cui affidare lo svolgimento delle attività di identificazione del Soggetto, registrazione e emissione.

Tali attività vengono demandate agli **Operatori di Registrazione (RAO/ODR).**

Gli **Incaricati alla Registrazione** svolgono esclusivamente attività di identificazione del Soggetto.

Entrambi operano sulla base delle istruzioni ricevute dalla RA, cui fanno riferimento e che ha compiti di vigilanza sulla correttezza delle procedure attuate.

1.3.3 Soggetto

Il **Soggetto** è la persona fisica o giuridica titolare del certificato qualificato, all'interno del quale sono inseriti i dati identificativi fondamentali. In alcune parti del Manuale e in alcuni limiti d'uso può essere definito anche Titolare.

1.3.4 Utente

È colui 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 elettronica qualificata 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 o ad una sua RA il rilascio di certificati digitali per un Soggetto, eventualmente sostenendone i costi e assumendo la facoltà di sospendere o revocare i certificati stessi.

Nello specifico si individuano le seguenti casistiche:

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

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

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 qualificati stabiliti nel territorio italiano al fine di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

1.3.6.2 Organismo di valutazione della conformità - Conformity Assessment Body

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

1.4 Uso del certificato

1.4.1 Usi consentiti

I certificati emessi dalla CA InfoCamere, secondo le modalità indicate dal presente Manuale Operativo, sono Certificati Qualificati ai sensi del CAD e del Regolamento eIDAS e rispettano le "*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*" di cui al regolamento pubblicato da AgID nella sua ultima versione.

Il certificato emesso dalla CA sarà usato per verificare la firma qualificata o del sigillo elettronico del Soggetto cui il certificato appartiene.

InfoCamere mette a disposizione per la verifica delle firme alcuni prodotti disponibili sul sito del Certificatore stesso (https://id.infocamere.it). Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

1.4.2 Usi non consentiti

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel Manuale Operativo e 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 Contatti

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

InfoCamere S.C.p.A.

Responsabile del Servizio di Certificazione Digitale

Corso Stati Uniti, 14, 35127 Padova PD

Telefono: 049-8288111

Call Center: http://supporto.infocamere.it/

Web: https://www.id.infocamere.it

e-mail: qtsp@pec.infocamere.it

Il Soggetto o il Richiedente possono richiedere copia della documentazione a lui relativa facendone richiesta al certificatore, compilando e inviando il modulo disponibile sul sito https://id.infocamere.it. La documentazione verrà inviata in formato elettronico all'indirizzo di email indicato nel modulo.

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene approvato dal Responsabile dei Servizi di Certificazione.

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda e conforme allo standard 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.

Definizioni	
Autocertificazione	È la dichiarazione, rivolta alla CA, effettuata personalmente da colui che risulterà Soggetto del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità con assunzione delle responsabilità stabilite per legge.
CAB – Conformity Assessment Body (Organismo di valutazione della conformità)	Organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
CAR – Conformity Assessment Report (Relazione di valutazione della conformità)	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr eIDAS [1]).
Certificato di firma elettronica	Un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona (cfr eIDAS [1]).
Certificato di sigillo elettronico	Un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona (cfr eIDAS [1]).
Certificato OneShot	Si intende certificato qualificato di firma elettronica qualificata per procedura remota disciplinato nel presente Manuale Operativo le cui chiavi, una volta generate, sono disponibili solo nell'ambito di un dominio informatico ed esclusivamente per la transazione di firma per la quale è stato emesso. Immediatamente dopo al suo utilizzo la chiave privata viene distrutta. In questa categoria sono compresi anche certificati denominati short-term in ETSI 319 411-1 per i quali il periodo di validità è inferiore al tempo massimo per evadere una richiesta di revoca come specificato nel presente manuale.
Certificato qualificato di firma elettronica	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (cfr eIDAS [1]).
Certificato qualificato di sigillo elettronico (QSealC)	Un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III del Regolamento eIDAS (cfr eIDAS [1]).
Chiave di certificazione o chiave di root	Coppia di chiavi crittografiche utilizzate dalla CA per firmare i certificati e le liste dei certificati revocati o sospesi.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Soggetto, mediante la quale si appone la firma elettronica qualificata sul documento informatico (cfr CAD [2]).

Definizioni	
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma elettronica qualificata apposta sul documento informatico dal Soggetto (cfr CAD [2]).
Codice Utente di emergenza (ERC)	Codice di sicurezza consegnato al Soggetto per inoltrare la richiesta di sospensione o revoca di un certificato sui portali del TSP.
Convalida	Il processo di verifica e conferma della validità di una firma elettronica (cfr eIDAS [1]).
Dati di convalida	Dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1]).
Dati di identificazione personale	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr eIDAS [1]).
Dati per la creazione di una firma elettronica	I dati unici utilizzati dal firmatario per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica	Un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica qualificata (SSCD – secure system creation device o QSCD)	Un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS (cfr eIDAS [1]). L'iniziale Q sta a intendere che il dispositivo è qualificato.
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1]).
Firma automatica	Particolare procedura informatica di firma elettronica eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.
Firma digitale (digital signature)	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al 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]).
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (cfr eIDAS [1]).
Firma elettronica avanzata	Una firma elettronica che soddisfi i requisiti di cui all'articolo 26 del Regolamento eIDAS (cfr eIDAS [1]).
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr eIDAS [1]).
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse
Firmatario	Una persona fisica che crea una firma elettronica (cfr eIDAS [1]).

Definizioni	
Giornale di controllo	Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [9].
ID Scratch	Identificativo univoco della cartellina o busta virtuale inviata all'utente per attivazione dei certificati e contenente il codice ERC.
Identificazione elettronica	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]).
Lista dei certificati revocati o sospesi [Certificate Revocation List - CRL]	È una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel registro pubblico.
Manuale operativo [certificate practice statement]	Il Manuale operativo definisce le procedure che la CA applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr eIDAS [1]).
Online Certificate Status Protocol (OCSP)	Protocollo definito dallo IETF nella RFC 6960, consente alle applicazioni di verificare la validità del certificato in maniera più veloce e puntuale rispetto alla CRL, di cui condivide i dati.
OTP - One Time Password	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Soggetto in un momento immediatamente antecedente all'apposizione della firma elettronica qualificata. Può essere basato su dispositivi hardware o su procedure software.
Parte facente affidamento sulla certificazione	Una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario (cfr eIDAS [1]).
Prestatore di servizi fiduciari	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato (cfr eIDAS [1]).
Prestatore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr eIDAS [1]).
Prodotto	Un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari (cfr eIDAS [1]).
Pubblico ufficiale	Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

Definizioni	
Registro pubblico [Directory]	Il Registro pubblico è un archivio che contiene: ▪ tutti i certificati emessi dalla CA per i quali sia stata richiesta dal Soggetto la pubblicazione; ▪ la lista dei certificati revocati e sospesi (CRL).
Revoca o sospensione di un certificato	È l'operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
Ruolo	Il termine Ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del 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.
Servizio fiduciario	Un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1]).
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1]).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi (cfr eIDAS [1]).
Sigillo elettronico avanzato	Un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36 del regolamento eIDAS (cfr eIDAS [1]).
Sigillo elettronico qualificato	Un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici (cfr eIDAS [1]).
Stato Membro	Stato Membro dell'Unione Europea
Tempo Universale Coordinato [Coordinated Universal Time]:	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento (cfr eIDAS [1]).
Validazione temporale elettronica qualificata	Una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS (cfr eIDAS [1]).
WebCam	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

Acronimo	
AgID	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
CA	Certification Authority
CAB	Conformity Assessment Body – Organismo di valutazione della conformità
CAD	Codice dell'Amministrazione Digitale
CAR	Conformity Assessment Report – Relazione di valutazione della conformità
CC	Common Criteria
CIE	Carta di Identità Elettronica
CNS – TS-CNS	Carta Nazionale dei Servizi Tessera Sanitaria – Carta Nazionale dei Servizi
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguish Name
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smartcard, ma con superiori caratteristiche di memoria e di performance
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Incaricato alla Registrazione
ISO	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione
ITU	International Telecommunication Union: fondata nel 1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
IUT	Identificativo Univoco del Titolare: è un codice associato al Soggetto che lo identifica univocamente presso la CA; il Soggetto ha codici diversi per ogni certificato in suo possesso

Acronimo	
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati
NTR Code	National Trade Register Code
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
ODR	Operatore di Registrazione
OTP	OneTime Password
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Soggetto per accedere alle funzioni del dispositivo stesso
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse, processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto
PSP	Service Payment Provider (prestatore servizi di pagamento)
QSealC	Qualified electronic Seal Certificate
RA	Registration Authority – Autorità di Registrazione
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
RSA	Deriva dalle iniziali degli inventori dell'algoritmo: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SPID	Sistema Pubblico di Identità Digitale
SSCD – QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una firma elettronica Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X500	Standard ITU-T per i servizi LDAP e directory
X509	Standard ITU-T per le PKI

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Archiviazione

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

In caso di eventi disastrosi e quindi impossibilità a erogare i servizi, il sito id.infocamere.it è reso disponibile nel rispetto dei tempi di ripristino dichiarati dal Certificatore sul sito www.infocamere.it.

Inoltre per garantire la continuità del servizio di revoca dei certificati, potranno essere utilizzati i servizi diretti della CA, facendo riferimento al canale PEC e/o canali applicativi diretti.

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del manuale operativo

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative alla CA previste dalla legge sono pubblicate presso l'elenco dei certificatori (al link https://eidas.agid.gov.it/TL/TSL-IT.xml) e presso il sito web della Certification Authority (cfr. § 1.5.1).

2.2.2 Pubblicazione dei certificati

Il Soggetto o il Richiedente legale rappresentante della persona giuridica che voglia rendere pubblico il proprio certificato può farne richiesta inviando l'apposito modulo (disponibile sul sito https://id.infocamere.it), firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione. La richiesta di pubblicazione del certificato deve essere inoltrata all'indirizzo PEC del QTSP. Tale possibilità non è prevista per i certificati OneShot.

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 indicato nell'attributo del certificato "CRL distribution point"/"Punto di distribuzione CRL". 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 con frequenza variabile se sono subentrati dei cambiamenti.

InfoCamere si riserva di apportare modifiche al presente Manuale Operativo per esigenze tecniche o modifiche procedurali intervenute durante la gestione del servizio.

Se i cambiamenti sono importanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*). Per la pubblicazione del CPS si deve attendere il permesso di AgID.

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

Le CRLs vengono pubblicate ogni ora.

2.4 Controllo degli accessi agli archivi pubblici

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

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

Il Soggetto nel certificato è identificato con l'attributo Distinguished Name (DN) che, quindi, deve essere valorizzato e conforme allo standard X500. I certificati vengono emessi in conformità con quanto stabilito nella specifica RFC-5280 e nelle norme ETSI EN-319-412-1, EN-319-412-2, EN-319-412-3, EN-319-412-4, EN-319-412-5 e secondo le indicazioni della determinazione AgID 147/2019 [6].

Rispetto a quanto stabilito nella specifica RFC 5280, per i certificati emessi a persona fisica e giuridica gli standard ETSI EN 319 412-2 par. 4.2.4 e 319 412-3 par. 4.2.1 consentono una lunghezza maggiore per i campi givenName, surname, commonName.

In accordo a tale deroga sono stati individuati i seguenti limiti massimi: givenName 40 caratteri, surname 40 caratteri e commonName 81 caratteri.

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.

I nomi contenuti nei campi SubjectName e SubjectAlternativeName dei certificati sono comprensibili nel linguaggio naturale e dovranno essere significativi per consentire la corretta identificazione dei Titolari del certificato.

Nell'ipotesi in cui ci sia necessità di emettere certificati al fine di realizzare prove tecniche, saranno indicati dati fittizi nel campo DN o Subject (es. "Organizzazione test", "Nome test", "Cognome test") o parole che inequivocabilmente ne denotano l'invalidità (es. "TEST", "PROVA"), facendo risultare il certificato privo di valenza legale, escludendo ogni responsabilità da parte della CA InfoCamere circa il suo utilizzo.

3.1.3 Anonimato e pseudonimia dei richiedenti

Nel caso in cui sia richiesto di inserire nel certificato uno pseudonimo in luogo dei dati reali del Richiedente, la CA si riserva di valutare caso per caso l'ammissibilità della richiesta.

Poiché il certificato è qualificato, la CA conserverà le informazioni relative alla reale identità della persona per venti (20) anni dall'emissione del certificato stesso.

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCamere si attiene allo standard X500.

3.1.5 Univocità dei nomi

Soggetto persona fisica:

Per garantire l'univocità del Soggetto, nel certificato deve essere indicato il nome e cognome e un codice identificativo univoco.

Generalmente si utilizza il Tax Identification Number (TIN). Il TIN viene 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.

Per i cittadini italiani, il codice identificativo univoco è il Codice Fiscale.

Soggetto persona giuridica:

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 a scelta tra:

- VAT (Value Added Tax Code)
- NTR (National Trade Register)

Nel caso di persone giuridiche italiane utilizzare la Partita IVA o il Numero di Registro Imprese. Se l'organizzazione non è dotata né di partita IVA né di NTR, ma solamente del codice fiscale, è possibile utilizzare i due caratteri "CF" seguito da ":IT-" (esempio: CF:IT- 97735020584) come previsto dalla Determina AgID 147/2019 [6].

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

Di seguito sono descritte le procedure usate per l'identificazione del Soggetto o del Richiedente al momento della richiesta di rilascio del certificato qualificato.

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

InfoCamere 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 Identificazione dell'identità delle organizzazioni

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

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

3.2.3 Identificazione della persona fisica

Fermo restando la responsabilità della CA, l'identità del Soggetto può essere accertata dai soggetti abilitati ad eseguire il riconoscimento, attraverso le seguenti modalità conformi all'art. 24 eIDAS [1]:

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
1 DeVisu	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione (IR)	n/a
2 SignatureID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione (IR)	Utilizzo di una firma elettronica qualificata emessa da un Prestatore di Servizi Fiduciari Qualificato
3 AuthenticationID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione (IR)	Utilizzo di un mezzo di autenticazione elettronica preesistente
4 VideoID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione (IR)	n/a

3.2.3.1 Riconoscimento effettuato secondo la modalità 1 – De Visu

La modalità di identificazione De Visu prevede un incontro di persona tra il Soggetto e un incaricato a eseguire il riconoscimento.

Il Soggetto esibisce all'incaricato della CA, appositamente formato, uno o più documenti d'identificazione in originale e in corso di validità tra quelli elencati di seguito

- Carta d'identità
- Passaporto
- Patente di guida

Ai fini della verifica dell'identità l'incaricato della CA provvede ad effettuare un controllo anche formale sul documento d'identificazione del Soggetto.

Nell'Addendum [7] sono elencati i documenti di identità italiani e stranieri che sono ritenuti accettabili

ai fini della corretta identificazione del Soggetto nell'ambito dei processi di emissione di certificati qualificati di firma elettronica.

Per garantire l'univocità del Soggetto e del relativo nome, questi deve essere in possesso anche del codice identificativo univoco di cui al paragrafo 3.1.5. L'incaricato abilitato ad eseguire il riconoscimento può richiedere l'esibizione di documentazione che comprovi il possesso di tale identificativo univoco.

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

3.2.3.2 Riconoscimento effettuato secondo la modalità 2 - SignatureID

Nella **modalità 2 SignatureID** la Certification Authority InfoCamere si basa sul riconoscimento già effettuato da un'altra CA che emette certificati qualificati.

In questo caso, il Richiedente è stato già previamente identificato da un prestatore di servizi fiduciari qualificato, che ha rilasciato il certificato digitale e utilizzerà quest'ultimo, se ancora in corso di validità, per firmare il modulo di richiesta di emissione del certificato qualificato da parte di InfoCamere.

I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

3.2.3.3 Riconoscimento effettuato secondo la modalità 3 - AuthenticationID

Nella **modalità 3 AuthenticationID** la CA si basa su un mezzo di identificazione elettronica preesistente:

- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello elevato;
- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello significativo, a patto che fornisca una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica;
- 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, e questa sia confermata da un organismo di valutazione della conformità.

Nello specifico, relativamente allo Stato Italia vengono riconosciuti come mezzi di identificazione elettronica adatti al riconoscimento:

a) la CNS (Carta nazionale dei Servizi);

b) la TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi);

c) la CIE (Carta di Identità Elettronica)

d) Le identità digitali rilasciate nel contesto del sistema SPID di livello 2 o superiore.

Nei casi a),b),c) di cui sopra il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server (caso CIE). Il sistema recupera le informazioni anagrafiche

inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione in oggetto di richiesta.

Nel caso d), il Richiedente, utilizzando le credenziali SPID di livello 2 o superiore, è chiamato ad effettuare un'autenticazione su di un portale del Certificatore attraverso meccanismi del circuito SPID. L'accesso alla funzionalità di richiesta del certificato avviene mediante autenticazione di livello 2 o superiore previa l'utilizzo di credenziali SPID rilasciate dal Gestore dell'Identità.

In tali casi, infatti, l'identità del Richiedente è già stata previamente accertata da uno dei Fornitori dell'Identità Digitale SPID accreditato dall'Agenzia per l'Italia Digitale.

I dati di registrazione sono conservati esclusivamente in formato elettronico.

3.2.3.4 Riconoscimento effettuato secondo la modalità 4 - VideoID

Nella **modalità 4 VideoID** è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphone, tablet, etc.), una webcam e un sistema audio funzionante.

L'Incaricato alla Registrazione, adeguatamente formato, verifica l'identità del Soggetto o del Richiedente tramite il riscontro con uno o più documenti di riconoscimento in corso di validità, muniti di fotografia recente e riconoscibile e ricompresi nella lista dei documenti accettati di cui al paragrafo 3.2.3.1

È facoltà dell'Incaricato alla Registrazione sospendere o non avviare il processo di video-identificazione qualora la qualità dello stream audio o video, necessariamente a colori, sia insufficiente o ritenuta non adeguata a soddisfare i requisiti di cui all'Art. 24 del Regolamento UE n.910/2014 o dell'art 32 comma 3, lettera a) del CAD o escludere l'ammissibilità del documento utilizzato dal Soggetto o dal Richiedente se ritenuto carente delle caratteristiche elencate.

I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

3.2.4 Informazioni del Soggetto o del Richiedente non verificate

Il Soggetto può ottenere, ai sensi dell'art.28 del CAD, direttamente o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di informazioni relative a:

- Titoli e/o abilitazioni Professionali;
  In questo caso il Richiedente, salvo diversi accordi tra la CA e l'Ordine di appartenenza (ove applicabile), oltre alla documentazione e alle necessarie informazioni identificative, dovrà produrre anche documentazione idonea a dimostrare l'effettiva sussistenza della specifica qualifica (o abilitazione professionale), eventualmente attestandolo mediante autocertificazione ai sensi dell'art. 46 del DPR n.445/2000. Tale documentazione non dovrà essere anteriore di oltre 10 (dieci) giorni alla data di registrazione. Nel caso in cui la qualifica sia autocertificata da parte del Richiedente, nel certificato non saranno inserite informazioni sull'organizzazione a cui potrebbe essere associato il Richiedente. La denominazione ed il

codice identificativo (es. Partita IVA) dell'organizzazione saranno invece inserite nel certificato se tale organizzazione ha espressamente richiesto o autorizzato il rilascio del certificato, anche senza l'esplicita indicazione di una qualifica. In tal caso, la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Richiedente. La CA si riserva di subordinare l'inserimento nel certificato delle informazioni che rientrano in questa categoria alla stipula di appositi accordi con i singoli enti, cui compete la gestione e tenuta degli albi, elenchi e/o registri professionali, per la disciplina delle modalità di attestazione della qualifica del Titolare e l'adempimento di quanto previsto a loro carico in qualità di "Terzo Interessato":

- Poteri di Rappresentanza di persone fisiche;
- Poteri di Rappresentanza di persone giuridiche o appartenenza alle stesse;
- Esercizio di Funzioni Pubbliche, Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi.

La ragione sociale o la denominazione e il codice identificativo dell'**Organizzazione** saranno invece riportate nel certificato se essa ha autorizzato il rilascio del certificato al Soggetto, anche senza l'esplicita indicazione di un ruolo. In tale ipotesi la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Soggetto. La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni che hanno una forma giuridica definita.

Il certificato con il **Ruolo** è conforme a quanto indicato nella Determina AgID 147/2019 [6].

3.2.5 Validazione dell'autorità

La CA ovvero la RA verificano che le informazioni richieste, definite nei paragrafi 3.2.2 3.2.3 e 3.2.4, per l'identificazione siano veritiere e appartengano alla persona che stanno identificando; ne validano quindi la richiesta.

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

Il rinnovo del certificato consiste nella generazione di una nuova coppia di chiavi (da parte del titolare) ed emissione di un ulteriore certificato con gli stessi dati identificativi del Titolare e periodo di validità uguale al certificato in scadenza (da parte del certificatore).

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 qualificato di firma.

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

Il 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.

La richiesta di rinnovo va effettuata prima dello scadere del certificato, restando inteso che la validità del certificato oggetto di rinnovo decorrerà dalla data del rinnovo stesso.

Con il rinnovo dei certificati, il Soggetto accetta la continuità della prestazione contrattuale da parte della CA.

3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati a seguito di revoca

Dopo la revoca o la scadenza del certificato non è possibile eseguire il rinnovo del certificato, diventando quindi necessaria una nuova emissione secondo le modalità indicate nel §3.2.3.

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 digitalmente il modulo presente sul sito della CA https://id.infocamere.it (vd § 4.9).

La richiesta può essere fatta attraverso un form Internet, in tal caso il Soggetto si autentica fornendo i dati anagrafici, l'ID Scratch e il codice di emergenza consegnato in forma riservata al momento dell'emissione del certificato.

Se la richiesta viene fatta presso la Registration Authority, l'autenticazione del Soggetto avviene con le modalità previste per l'identificazione al paragrafo 3.2.3.1.

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 o un Terzo Interessato da cui derivano i poteri di firma del titolare 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 al paragrafo 4.9. La CA si riserva di individuare ulteriori modalità di inoltro della richiesta, di revoca o sospensione del Richiedente o del Terzo Interessato in apposite convenzioni da stipulare con

lo stesso.

4 OPERATIVITÀ

4.1 Richiesta del certificato

4.1.1 Chi può richiedere un certificato

Il certificato qualificato per una persona fisica può essere richiesto dal Soggetto rivolgendosi presso le RA del certificatore.

Il certificato qualificato per una persona giuridica può essere richiesto dal Richiedente rivolgendosi alla CA o 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 qualificato. Quando il Soggetto è una persona giuridica, tali responsabilità ricadono sul legale rappresentante o soggetto munito di apposita procura, che richiede il certificato qualificato;
- 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 il responsabile ultimo della identificazione del Soggetto e del buon esito del processo di iscrizione del certificato qualificato.

4.2 Elaborazione della richiesta

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

- prendere visione della documentazione contrattuale e dell'eventuale ulteriore

documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel paragrafo 3.2.3;
- 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 qualificato 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 TIN (codice fiscale nel contesto italiano)
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- I dati di contatto per l'invio delle comunicazioni dalla CA al Soggetto,
  - Indirizzo di residenza
  - Indirizzo e-mail;
- numero di telefonia mobile, per comunicazioni dalla CA al Soggetto e per la trasmissione della OTP ove fosse questa la tecnologia OTP adottata.

In fase di richiesta, il Richiedente deve dimostrare di essere in possesso esclusivo dell'indirizzo e-mail e del numero di telefonia mobile tramite codice di validazione inviato. L'indirizzo e-mail sarà usato per comunicazioni dalla CA e per l'invio dei codici di emergenza (ERC) e, ove previsto, gli avvisi di scadenza. Questa considerazione non è applicata nei casi di certificati One-Shot.

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.

4.2.1.2 Persona giuridica

Per la richiesta di un certificato qualificato 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 TIN o analogo codice identificativo del Richiedente (codice fiscale per il contesto

italiano);

- 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;
- numero di telefonia mobile, per comunicazioni dalla CA al Richiedente e per la trasmissione della OTP ove fosse questa la tecnologia OTP adottata;
- Nome del Soggetto persona giuridica;
- VAT code ovvero NTR (partita IVA o numero di Registro Imprese per i Soggetti italiani).

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

4.2.1.3 Registrazione

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 all'attivazione del dispositivo di firma o della procedura di firma, se remota, sia alla eventuale richiesta di sospensione/riattivazione/revoca del certificato (codice ERC o codice analogo, se previsto dal contratto). I codici di sicurezza sono consegnati in busta cieca ovvero, se elettronici, trasmessi all'interno di file cifrati.

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

La CA può prevedere inoltre che il certificato di firma per procedura remota sia utilizzabile ai fini della sottoscrizione dei documenti provenienti da specifiche procedure definite dal Certificatore o ulteriori procedure esterne che fanno utilizzo di API di integrazione dallo stesso gestite, previa analisi delle caratteristiche del sistema nell'ambito del perimetro di certificazione del dispositivo sicuro di firma.

4.2.2 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.

4.2.3 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

L'emissione del certificato fa seguito ad una richiesta presentata secondo le modalità e fornendo le informazioni descritte nei par. 3.2 e 4.1, attraverso un processo articolato in diverse fasi e basato su canali di comunicazione sicuri.

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

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

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

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

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

Il Soggetto o il Richiedente si autenticano ai servizi o alle applicazioni messe a disposizione dalla CA.

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

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

4.3.1.3 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 qualificato di sottoscrizione per procedura automatica specificatamente autorizzato a tal fine.

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

Il Servizio prevede la gestione in forma remota da parte del Richiedente del certificato qualificato di sigillo elettronico, ai fini della sottoscrizione dei documenti provenienti da specifiche procedure

definite dal Certificatore o ulteriori procedure esterne che fanno utilizzo di API di integrazione dallo stesso gestite previa analisi delle caratteristiche del sistema nell'ambito del perimetro di certificazione del dispositivo sicuro di firma.

4.3.1.4 Emissione del certificato con finalità di test

Nei casi previsti o per necessità di effettuare test in ambiente di produzione, la procedura di emissione di certificati viene eseguita sottostando a tali vincoli:

- I dati utilizzati per la registrazione devono indicare inequivocabilmente nel campo Subject che si tratti di un certificato di test e non di un certificato effettivo, secondo quanto riportato nel § 3.1.2
- L'Ufficio di registrazione utilizzato deve essere un ufficio interno ad InfoCamere o inequivocabilmente riconducibile all'uso esclusivo di test (es. contenente le parole prova, test, ecc. nella denominazione)
- Nel momento in cui si conclude la sessione di test, il certificato deve essere revocato d'ufficio.

Eventuali eccezioni sull'utilizzo di nomi veri o di uffici di registrazioni afferenti ad un Cliente devono essere concordate con il Responsabile della CA.

In tutti i casi il certificato deve essere revocato d'ufficio nel momento in cui non dovesse più servire.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

L'avvenuta emissione del certificato viene notificata all'operatore di registrazione, che consegna il dispositivo al Titolare nel caso di riconoscimento DeVisu, e, in ogni caso, al Titolare stesso tramite l'indirizzo email che ha indicato al momento della richiesta.

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 gli appositi software messo a disposizione dalla CA, procede ad attivare il dispositivo scegliendo contestualmente il PIN di firma, la cui custodia e tutela è posta esclusivamente in capo al Soggetto stesso.

In alcuni casi il certificato può essere emesso già attivo e utilizzabile tramite i codici ricevuti in maniera riservata.

4.3.3.2 Attivazione del dispositivo di firma remota (HSM)

Il Soggetto, ovvero il Richiedente in caso di persona giuridica, autenticato ai portali della CA attraverso i codici di attivazione ricevuti in maniera riservata, sceglie la password di firma, quantità di sicurezza

riservata la cui custodia e tutela è posta esclusivamente in capo al Soggetto o al Richiedente stesso, che viene confermato con l'inserimento della OneTime Password ricevuta via SMS.

4.4 Accettazione del certificato

4.4.1 Comportamenti concludenti di accettazione del certificato

n/a

4.4.2 Pubblicazione del certificato da parte della Certification Authority

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

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 adottare misure di sicurezza atte a prevenire l'utilizzo non autorizzato della chiave privata, conservandola separatamente dal dispositivo e non cedendola o concedendola in uso in nessuna circostanza a soggetti terzi. Deve garantire la protezione della segretezza e la conservazione del codice di emergenza, 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

I certificati qualificati di sottoscrizione per procedura automatica contengono il limite d'uso previsto dall'Autorità di Vigilanza, come ulteriori Certificate Policy:

- Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.
- I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.

I certificati emessi sulla base dell'identificazione di tipo 3 AuthenticationID attraverso il nodo eIDAS, utilizzando identità digitali SPID, contengono l'OID 1.3.76.16.5 e il seguente limite d'uso in ottemperanza all'avviso n° 17 del 24 gennaio 2019:

- Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity

I certificati di Firma Digitale One-Shot riportano il seguente limite d'uso:

- L'utilizzo del certificato è limitato applicativamente alla sottoscrizione dei documenti cui la firma è apposta. The use of the certificate is technically limited to the signature of the underlying documents.

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

È inoltre facoltà del Soggetto o del Richiedente richiedere alla Certification Authority l'inserimento nel certificato di limiti d'uso personalizzati (max 200 caratteri). 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.

4.6 Rinnovo del certificato

4.6.1 Motivi per il rinnovo

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

La procedura di rinnovo è prevista solo per i certificati a persona fisica emessi su smart card o token. In tutti gli altri casi sarà necessario procedere ad una nuova emissione.

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 e se tutte le informazioni fornite all'atto della prima emissione sono ancora valide; oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla richiesta di un nuovo certificato secondo le modalità riportate al §3.2.3.

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

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.

L'informazione sullo stato di revoca rimane disponibile presso la Certification Authority per 20 anni dopo la scadenza del certificato di root CA tramite l'emissione e conservazione a mezzo dei servizi di Conservazione a norma dell'ultima CRL.

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 di chi la richiede.

4.9.3.1 Revoca richiesta dal Soggetto

Il Soggetto può richiedere la revoca del certificato:

1. utilizzando la funzione di revoca disponibile 7x24 nel sito web della CA, indicando i dati richiesti e utilizzando l'ID scratch e il codice di emergenza fornito in sede di emissione del certificato;
2. tramite la Registration Authority, la quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la revoca alla CA. Il Soggetto è tenuto a sottoscrivere la richiesta di revoca e consegnarla alla RA, corredata di una scansione di un documento di identità in corso di validità;
3. inviando alla CA, all'indirizzo PEC del QTSP, il modulo presente nel sito id.infocamere.it, compilato e allegando la scansione di un documento di identità in corso di validità.

La CA o RA verificano l'autenticità della richiesta, avvalendosi - nei casi al punto 2 e 3 - della facoltà di richiedere documentazione integrativa, poi procedono 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.

Per la definizione stessa del certificato short-term, non è prevista la richiesta della revoca dei certificati short-term da parte del Soggetto.

4.9.3.2 Revoca richiesta dal Richiedente o dal Terzo Interessato

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

La CA o RA verificano l'autenticità della richiesta in modo che la CA possa procedere alla revoca del certificato; subito dopo ne dà notizia al Soggetto utilizzando il mezzo di comunicazione stabilito all'atto della richiesta 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.

Per la definizione stessa del certificato short-term, non è prevista la richiesta della revoca dei certificati short-term da parte del Richiedente.

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, salvo casi d'urgenza, 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.

In casi eccezionali, la CA può revocare anche i certificati short-term, comunicandolo preventivamente al Soggetto e al Richiedente, fornendo il motivo della revoca, nonché la data e l'ora di decorrenza.

4.9.4 Periodo di grazia della richiesta di revoca

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

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

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

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dalla CA, e pubblicata nel Registro pubblico. La CRL viene pubblicata in modo programmato ogni ora (emissione ordinaria). La CA può, in circostanze particolari, forzare un'emissione non programmata della CRL (emissione straordinaria immediata), ad esempio nel caso in cui la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata). La CRL è emessa sempre integralmente. Il momento della pubblicazione della CRL viene attestata utilizzando quale riferimento temporale la data fornita dal sistema di Time Stamping Authority InfoCamere 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, InfoCamere mette a disposizione anche un servizio OCSP per la verifica dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 X 7.

La coerenza tra il servizio OCSP e la CRL è garantita entro massimo un'ora. La coerenza del servizio OCSP e dell'aggiornamento delle informazioni emesse dal servizio stesso in relazione agli aggiornamenti della CRL è vincolata dal tempo di attesa necessario all'aggiornamento della CRL stessa come definito nel paragrafo che precede.

4.9.10 Requisiti servizi online di verifica

Si veda Appendice B

4.9.11 Altre forme di revoca

n/a

4.9.12 Requisiti specifici rekey in caso di compromissione

n/a

4.9.13 Motivi per la sospensione

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

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il Soggetto, il Richiedente o Terzo Interessato, la RA o la CA hanno acquisito elementi di dubbio sulla validità del certificato;
3. siano insorti dubbi sulla sicurezza del dispositivo OTP, qualora presente;
4. è necessaria un'interruzione temporanea della validità del certificato.

In caso di sospetto furto di identità, la CA, senza preavviso, potrà procedere a una sospensione cautelativa.

Nei casi citati si richiederà la sospensione del certificato specificandone la durata; alla scadenza di tale periodo ed entro la scadenza naturale del certificato stesso, 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 o dal Terzo Interessato, per i motivi e nelle modalità previsti dal presente Manuale Operativo. Infine, il certificato può essere sospeso d'ufficio dalla CA.

4.9.15 Procedure per richiedere la sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda di chi la richiede.

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 7x24 nel sito web della CA, indicando i dati richiesti e utilizzando l'ID scratch e il codice di emergenza fornito in sede di emissione del certificato;
2. prenotando un appuntamento telefonico con il Call Center della CA;
3. tramite la Registration Authority, la quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione alla CA. Il Soggetto è tenuto a sottoscrivere la richiesta di sospensione e consegnarla alla RA, corredata di una scansione di un documento di identità in corso di validità.
4. inviando alla CA, all'indirizzo PEC del QTSP, il modulo presente nel sito id.infocamere.it,

compilato e allegando la scansione di un documento di identità in corso di validità.
Nei casi indicati al punto 3 e 4 la CA o RA si riservano la facoltà di richiedere documentazione integrativa prima di procedere alla sospensione del certificato.
La CA, qualora nel certificato oggetto della richiesta di 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 richiesta di sospensione sia presente l'indicazione dell'Organizzazione, provvederà a comunicare l'avvenuta sospensione a tale soggetto.

Per la definizione stessa del certificato short-term, non è prevista la richiesta della sospensione dei certificati short-term da parte del Soggetto.

4.9.15.2 Sospensione richiesta dal Richiedente o dal Terzo Interessato

Il Richiedente o il Terzo Interessato possono richiedere la sospensione del certificato del 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.

Per la definizione stessa del certificato short-term, non è prevista la richiesta della sospensione dei certificati short-term da parte del Richiedente.

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 ed eventualmente 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

La procedura di sospensione provoca l'interruzione temporanea della validità del certificato fino alla sua naturale scadenza o fino alla presentazione di una richiesta di riattivazione o revoca.

Qualora la sospensione sia mantenuta fino al giorno di scadenza del certificato, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

È possibile richiedere la riattivazione del certificato prima della data del termine di sospensione utilizzando le medesime procedure indicate al §4.9.15.

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 sono disponibili 24 ore per 7 giorni la settimana.

4.10.3 Caratteristiche opzionali

n/a

4.11 Disdetta dai servizi della CA

Il rapporto del 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

Il TSP InfoCamere 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 il TSP 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 InfoCamere è disponibile facendone richiesta alla casella PEC **qtsp@pec.infocamere.it**

Le politiche di sicurezza in InfoCamere sono sottoposte a review non meno che annualmente, vengono inoltre aggiornate a fronte di ogni cambiamento significativo. Ogni review viene tracciata all'interno del documento stesso anche quando non sia stato necessario apportare alcuna modifica.

5.1 Sicurezza fisica

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

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

5.1.1 Posizione e costruzione della struttura

Il Data Center InfoCamere si trova presso la sede operativa di Padova. Il sito di Disaster Recovery è ubicato a Ponte San Pietro (Bergamo) 1 Gbit/s upgradabile fino a 10 Gbit/s.

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

5.1.2 Accesso fisico

L'accesso al Data Center è regolato dalle procedure InfoCamere 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 che ospita il Data Center InfoCamere su Padova, pur non essendo certificato, ha le caratteristiche di un Data Center di tier 3.

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

L'infrastruttura preposta all'alimentazione include:

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

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

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

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

5.1.4 Prevenzione e protezione contro gli allagamenti

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

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

5.1.5 Prevenzione e protezione contro gli incendi

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

L'impianto di rilevazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici NAFS125 e PF23 e, in alcune sale, con sistemi di spegnimento ad aerosol.

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

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

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

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

InfoCamere è certificata ISO 14001 per la gestione ambientale sostenibile del proprio ciclo produttivo, compresa la raccolta differenziata e lo smaltimento sostenibile dei rifiuti. Per quel che riguarda il contenuto informativo dei rifiuti elettronici, tutti i media, prima della dismissione, vengono ripuliti secondo le procedure previste ovvero avvelandosi di società di sanitizzazione certificate.

5.1.8 Off-site backup

L'off-site backup è realizzato nel sito di Disaster Recovery a Ponte San Pietro (Bergamo): i server sono replicati tramite tecnologia di Veeam Backup & Replication, poggiano su 2 infrastrutture distinte sia a livello fisico che logico, una per la CA ed una per il resto dei servizi.

Gli HSM presenti nel sito di DR sono stati inizializzati nella medesima modalità della produzione, in modo da poter erogare il servizio in caso di necessità.

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 caratteristiche e 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 competenze 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 InfoCamere 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

Tutto il personale, riceve un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.

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 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 i primi mesi dell'anno il Piano Formativo così definito viene condiviso e reso pubblico.

5.3.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede viene regolata attraverso un piano di turnazione che viene predisposto dal responsabile di unità organizzativa mensilmente, con un anticipo di almeno 10 giorni. Ogni turno ha una durata di 8 ore lavorative.

Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicendare nel lavoro a turni il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

Non sono previsti turni di presenza in sede notturni. I turni di presenza in sede avvengono su una fascia oraria dalle ore 07:00 alle ore 21:00 dal lunedì al venerdì e dalle 07:00 alle 12:00 il sabato.

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.

5.3.7 Controlli sul personale non dipendente

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

5.3.8 Documentazione fornita al personale

Il Certificatore assicura a tutto il personale impiegato nell'ambito dei servizi di CA,la disponibilità di tutta la documentazione necessaria per il corretto svolgimento delle loro mansioni (questo CPS, le procedure operative, la modulistica, le guide, le policy di sicurezza, ecc.).

Il personale dovrà invece prendere visione del Codice Etico InfoCamere.

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.

5.4.1 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 documento 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.

Vengono registrati tutti gli accessi fisici ai locali ad alta sicurezza dove risiedono le macchine della CA.

Vengono registrati tutti gli accessi logici alle applicazioni della CA.

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

5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo

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

5.4.3 Periodo di conservazione del giornale di controllo

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

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita, secondo la normativa vigente, da Sistema di Conservazione a norma.

5.4.5 Procedure di backup del giornale di controllo

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

5.4.6 Sistema di memorizzazione del giornale di controllo

La raccolta dei log degli eventi avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dal sistema di conservazione a norma e descritto nel manuale della sicurezza del suddetto sistema.

5.4.7 Notifica in caso di identificazione di vulnerabilità

n/a

5.4.8 Valutazioni di vulnerabilità

InfoCamere 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 la totalità dei servizi.

5.5 Archiviazione dei verbali

5.5.1 Tipi di verbali archiviati

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

5.5.2 Protezione dei verbali

La protezione è garantita dal Sistema di Conservazione dei documenti InfoCamere, 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 della sicurezza del suddetto sistema.

5.5.4 Requisiti per la marcatura temporale dei verbali

n/a

5.5.5 Sistema di memorizzazione degli archivi

La raccolta dei verbali avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dal sistema di conservazione a norma InfoCamere e descritto nel manuale della sicurezza del suddetto sistema.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

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

5.6 Sostituzione della chiave privata della CA

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

5.7 Compromissione della chiave privata della CA e disaster recovery

5.7.1 Procedure per la gestione degli incidenti

La CA ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27000. 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 InfoCamere; 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 InfoCamere conforme all'articolo 19 del Regolamento[1].

5.7.2 Corruzione delle macchine, del software o dei dati

In caso di guasto del dispositivo sicuro di firma HSM contenente le chiavi di certificazione si fa ricorso alla copia di riserva della chiave di certificazione, opportunamente salvata e custodita, e non vi è necessità di revocare il corrispondente certificato della CA.

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

5.7.3 Procedure in caso di compromissione della chiave privata della CA

La compromissione della chiave di certificazione è considerato un evento particolarmente critico, in quanto invaliderebbe i certificati emessi firmati con tale chiave. Vi è quindi una particolare attenzione alla protezione della chiave di certificazione e a tutte le attività di sviluppo e manutenzione del sistema che possono avere impatto sulla stessa.

InfoCamere ha descritto la procedura da seguire in caso di compromissione della chiave, nell'ambito del SGSI certificato ISO 27000.

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

- a informare il Supervisory Body italiano AgID per la rimozione della chiave dalla TSL e il CAB,
- ad avvisare le RA e i clienti, siano essi soggetti del certificato o richiedenti, tramite comunicazione diretta, ove possibile, e tramite comunicazione sul sito,

a revocare i certificati impattati, a procedere eventualmente all'emissione e accreditamento di una nuova root CA e a fornire in maniera affidabile le informazioni sullo stato di revoca dei certificati.

5.7.4 Erogazione dei servizi di CA in caso di disastri

InfoCamere 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, InfoCamere comunicherà questa intenzione all'Autorità di vigilanza (AgID) e l'ente di certificazione (CAB) con un anticipo di almeno 6 mesi, indicando, eventualmente, il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione. Con pari anticipo InfoCamere 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.

In caso di cessazione della CA l'informazione sullo stato di revoca sarà fornita tramite l'emissione di un'ultima CRL, come previsto dallo standard ETSI EN 319 411-1.

I dettagli di tale procedura sono presenti nel documento non pubblico "Termination Plan servizi di CA", disponibile presso il Certificatore.

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 anche di tipo HSM utilizzando le funzionalità native offerte dai dispositivi stessi.

6.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico, sia esso un SSCD o un QSCD. Per i certificati di firma remota e automatica il dispositivo crittografico è sempre un HSM. 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. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 4096 bits.

Per le chiavi del soggetto l'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è non inferiore a 2048 bits.

6.1.6 Controlli di qualità e generazione della chiave pubblica

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il § 6.2.1) e garantiscono che la chiave pubblica sia corretta e randomica.

6.1.7 Scopo di utilizzo della chiave

6.1.7.1 Utilizzo chiave di CA

La chiave di CA viene utilizzata solamente per la firma dei certificati dei Titolari, delle Liste di Revoca e dei certificati OCSP. L'estensione KeyUsage del certificato di CA contiene firma certificati (keyCertSign) e firma CRL (cRLSign).

Le risposte OCSP sono firmate tramite appositi certificati con extKeyUsage valorizzato con ocspSigning.

6.1.7.2 Utilizzo chiave del Titolare

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

6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

6.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da InfoCamere per le chiavi di certificazione (CA) e per il risponditore OCSP sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in Europa.

Le smart card utilizzate da InfoCamere sono validate Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) ovvero EAL5 Augmented by ALC_DVS.2 , AVA_VAN.5 .

I moduli crittografici utilizzati da InfoCamere per le chiavi di firma remota e automatica del Soggetto sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4.

6.2.2 Controllo di più persone della chiave privata di CA

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

6.2.3 Deposito presso terzi della chiave privata di CA

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 dl personale che ha accesso ai dispositivi sia di chi ha l'accesso alla cassaforte.

6.2.5 Archiviazione della chiave privata di CA

n/a

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

n/a

6.2.7 Memorizzazione della chiave privata su modulo crittografico

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

6.2.8 Metodo di attivazione della chiave privata

La chiave privata di certificazione viene attivata dal software della CA in dual control, cioè due persone con ruoli specifici e in presenza del responsabile del servizio.

Il Soggetto o il Richiedente legale rappresentante della persona giuridica è responsabile di proteggere la propria chiave privata con una password robusta per prevenire l'utilizzo non autorizzato. Per attivare la chiave privata, il 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 InfoCamere deputato a questo ruolo si occupa della distruzione della chiave privata quando il certificato è scaduto o revocato, secondo le procedure di sicurezza previste dalle politiche di sicurezza e le specifiche del produttore del dispositivo.

6.2.11 Classificazione dei moduli crittografici

n/a

6.3 Altri aspetti della gestione delle chiavi

n/a

6.3.1 Archiviazione della chiave pubblica

n/a

6.3.2 Periodo di validità del certificato e della coppia di chiavi

Il periodo di validità del certificato è determinato sulla base:

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

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

3.3.1.

Attualmente il certificato della CA ha una durata di 16 anni, i certificati emessi a persona fisica o giuridica hanno validità non superiore ai 39 mesi.

6.4 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.3.3 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), ossia configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della CA.

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

6.6 Operatività sui sistemi di controllo

InfoCamere 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.

InfoCamere è certificata UNI CEI EN ISO/IEC 27001:2017 per le attività EA:33-35 con le estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:201 per i servizi in cloud. La prima certificazione ISO/IEC 27001:2005 risale al 2012.

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 InfoCamere.

6.7 Controlli di sicurezza della rete

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

6.8 Sistema di validazione temporale

InfoCamere fornisce un servizio di validazione temporale qualificato. Per la marcatura temporale fare riferimento al manuale operativo IC-MO-TSA presente sul sito del prestatore di servizi fiduciari InfoCamere.

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 [1] e alla Determinazione AgID n.147/2019 [6]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.

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

In Appendice A 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 InfoCamere sono X.509 versione 3.

7.1.2 Estensioni del certificato

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

Per le estensioni del certificato si veda Appendice A.

7.1.3 OID dell'algoritmo di firma

I certificati sono firmati con il seguente algoritmo:

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

7.1.4 Forme di nomi

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

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2.

7.2 Formato della CRL

Per formare le liste di revoca CRLs, InfoCamere 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 InfoCamere sono X.509 versione 2.

7.2.2 Estensioni della CRL

Per le estensioni della CRL si veda Appendice A.

7.3 Formato dell’OCSP

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

7.3.2 Estensioni dell’OCSP

Per le estensioni dell’OCSP si veda Appendice A.

8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e non, in conformità al Regolamento eIDAS è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento.

InfoCamere ha presentato ad AgID l'apposita richiesta per ottenere il riconoscimento di "prestatore del servizio fiduciario qualificato" allegando un report della valutazione di conformità con il Regolamento (Conformity Assesment Report - CAR) rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.

InfoCamere presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 del 23/07/2014, sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319_403 e UNI CEI EN ISO/IEC 17065:2012.

8.1 Frequenza o circostanze per la valutazione di conformità

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

8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

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

8.3 Rapporti tra InfoCamere e CAB

InfoCamere e CSQA non hanno interessi finanziari né relazioni di affari.

Non sono in corso rapporti commerciali o di partnership che possono creare pregiudizi a favore o contro InfoCamere nella valutazione obiettiva di CSQA.

8.4 Aspetti oggetto di valutazione

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

8.5 Azioni in caso di non conformità

In caso di non conformità, il CAB deciderà se inviare comunque il rapporto ad AgID, o se riservarsi di rieseguire l'audit dopo che la non conformità sia stata sanata.

InfoCamere 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 https://id.infocamere.it e/o presso il sito web delle Registration Authority. La CA può stipulare accordi commerciali con le RA e/o i Richiedenti prevedendo tariffe specifiche.

9.1.2 Tariffe per l'accesso ai certificati

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

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

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

9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili presso il sito https://id.infocamere.it o presso il sito web delle Registration Authority.

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

9.1.5 Politiche per il rimborso

Il recesso e il relativo rimborso è disciplinato dalle Condizioni Generali di Contratto dei Servizi di Certificazione e dalle Condizioni Generali Certificato a persona giuridica per Sigillo Elettronico, pubblicate sul sito https://id.infocamere.it. Le istruzioni operative per l'esercizio del diritto di recesso e la richiesta di rimborso sono disponibili al sito della CA o presso le RA.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Il TSP InfoCamere ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato trattato ed accettato da AgID, che ha come massimali:

- 10.000.000 euro per singolo sinistro;
- 10.000.000 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 InfoCamere in conformità a quanto indicato nel Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm. ii. e nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018 [3].

9.4.1 Programma sulla privacy

InfoCamere 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 [3]; per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome o un numero di identificazione.

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 dei dati personali

InfoCamere S.C.p.A.

Sede Legale: Via Giovanni Battista Morgagni, 13, 00161 Roma

9.4.5 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy dei servizi fiduciari è disponibile sul sito id.infocamere.it

Prima di eseguire ogni trattamento di dati personali, InfoCamere procede a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge [3].

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

9.6 Rappresentanza e garanzie

9.6.1 Certification Authority

La CA si impegna ad erogare il servizio in conformità con quanto prescritto nel presente Manuale Operativo e a rilasciare una copia dello stesso a chiunque ne faccia richiesta; a fornire informazioni chiare e complete sullo stato dei certificati e sulle condizioni del servizio nonché ad assicurare un efficiente servizio di sospensione e revoca dei certificati.

La CA si impegna altresì a rispettare tutti gli obblighi previsti all'art. 32 del CAD.

La CA tratta i dati personali secondo quanto previsto dall'informativa di cui all'articolo 13 del Regolamento (UE) 2016/679 mantenendo inoltre la responsabilità per l'osservanza delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto, ai sensi dell'art. 2.4.1. dell'Allegato al Regolamento di esecuzione UE 2015/1502 della Commissione.

9.6.2 Registration Authority

Nel caso di specie la rappresentanza si esplica tramite mandato conferito da InfoCamere all'Ufficio di Registrazione (RA), nel quale vengono definiti il regime di responsabilità e gli obblighi delle parti. In particolare, l'Ufficio di Registrazione si impegna a svolgere l'attività di registrazione nel rispetto della normativa vigente e delle procedure di cui ai Manuali Operativi, con particolare riferimento all'identificazione personale certa di coloro che sottoscrivono la richiesta di certificazione digitale ed a trasmettere i risultati di tali attività ad InfoCamere.

9.6.3 Titolare

Il Titolare è responsabile della veridicità dei dati comunicati nel modulo di richiesta. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, sarà considerato responsabile di tutti i danni derivanti al Certificatore e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare il Certificatore da eventuali richieste di risarcimento danni. Il Titolare ed il Richiedente sono altresì responsabili dei danni derivanti al Certificatore e/o a terzi nel caso di ritardo da parte loro dell'attivazione delle procedure previste nel punto 4.9 del presente Manuale (revoca e sospensione del certificato).

9.6.4 Relying Party

Con il termine Relying Party ci si riferisce a tutti quei soggetti che fanno affidamento sulle informazioni contenute nel certificato. Questi soggetti devono in particolare verificare l'autenticità e l'integrità del certificato; verificare che il certificato non sia sospeso revocato o scaduto; tenere in considerazione la qualifica del titolare, organizzazione di appartenenza del titolare, limiti d'uso, limiti di valore (se presenti nel certificato).

9.6.5 Altri soggetti

Ai sensi delle norme vigenti (in particolare [2]), il "Terzo Interessato" è la persona fisica o giuridica che acconsente all'inserimento di una qualifica nel certificato oppure l'organizzazione che richiede o autorizza il rilascio del certificato del titolare.

Il Terzo Interessato è tenuto a conoscere il presente Manuale Operativo e a informare tempestivamente la CA nel caso in cui le condizioni in essere al momento della emissione del certificato (per es. il possedere, da parte del Titolare, determinate qualifiche professionali o il suo appartenere alla suddetta organizzazione o il suo ricoprire in essa determinate cariche) vengano meno, richiedendo in tal caso la revoca del certificato.

9.7 Limitazioni di garanzia

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

Il Certificatore garantisce unicamente il funzionamento del Servizio, secondo i livelli indicati al paragrafo 9.17 del presente Manuale Operativo.

9.8 Limitazioni di responsabilità

Il Certificatore non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti e/o, eventualmente, degli *hash* trasmessi dalla procedura informatica indicata dal Richiedente o dal Titolare, non assumendo alcuna responsabilità, in merito alla validità e riconducibilità degli stessi all'effettiva volontà del Titolare.

Fatto salvo il caso di dolo o colpa, il Certificatore non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificati di sottoscrizione rilasciati in base alle previsioni del presente Manuale, delle "Condizioni Generali – Servizi di Certificazione" e delle "Condizioni Generali - Certificato a Persona Giuridica per Sigillo Elettronico".

InfoCamere non è responsabile di qualsiasi danno diretto e/o indiretto derivante in via anche alternativa (i) dalla perdita, (ii) dalla impropria conservazione, (iii) da un improprio utilizzo, degli strumenti di identificazione e di autenticazione e/o (iv) dalla mancata osservanza di quanto sopra, da parte del Titolare.

Il Certificatore, inoltre, fin dalla fase di formazione delle "Condizioni Generali – Servizi di Certificazione" e delle "Condizioni Generali - Certificato a Persona Giuridica per Sigillo Elettronico", e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e della rete internet.

InfoCamere, salvo il caso di dolo o colpa, non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Titolare, al Richiedente e/o a terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati da parte di terzi non autorizzati da InfoCamere.

9.9 Indennizzi

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

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

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo improprio del servizio di certificazione o al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili ad InfoCamere, quali, a titolo esemplificativo, scioperi, sommosse, terremoti, atti di terrorismo, tumulti popolari, sabotaggio

organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari hardware e/o dei software utilizzati dal Richiedente.

9.10 Termine e risoluzione

9.10.1 Termine

Al termine del rapporto tra CA e Soggetto o tra CA e Richiedente, il certificato viene revocato. I Contratti "Condizioni Generali – Servizi di Certificazione" e "Condizioni Generali- Certificato a Persona Giuridica per Sigillo Elettronico" (di seguito "il Contratto") intercorrenti tra il Certificatore e il Soggetto ha durata pari a quella del certificato di sottoscrizione indicata nel campo "validità (*validity*)" dello stesso.

Prima della scadenza, il Titolare può richiedere il rinnovo del certificato, secondo la procedura indicata dal presente Manuale Operativo. Il rinnovo comporta la proroga del Contratto fino alla scadenza o revoca del certificato rinnovato ed il pagamento dei corrispettivi stabiliti per tale servizio.

9.10.2 Risoluzione

La risoluzione e il recesso delle parti è regolato dalle Condizioni Generali - Servizi di Certificazione pubblicate sul sito https://id.infocamere.it.

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata revoca del certificato.

9.11 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1

9.12 Revisione del Manuale Operativo

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

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio

modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo Manuale Operativo verrà prontamente comunicata alle RA.

Se i cambiamenti sono rilevanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

9.12.1 Storia delle revisioni

Versione	Data	Modifiche
1	10/02/2020	Prima versione del documento
2	28/04/2021	Intero documento: correzioni refusi Introduzione § 3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati a seguito di revoca Integrazioni al § 4.2.1.1: indicazione univocità del contatto email associato al Titolare § 4.9.13 sospensione cautelativa da parte della CA
3	27/07/2021	§3.2.3.3 Aggiunti ulteriori mezzi di identificazione elettronica modalità 3 – AuthenticationID §4.5.3 Aggiunto limite d'uso per emissione con SPID e aggiornata descrizione limite di valore Rivisti i §9.1.5 Politiche per il rimborso, §9.10.2 Risoluzione, §9.14 Foro competente
4	16/12/2022	Intero documento: revisione annuale § 4.3.1.4 Emissione del certificato con finalità di test §3.2.3.1 e §9.15 Inserito riferimento ad "Allegato al Manuale Operativo / Certificate Policy e Certificate Practice Statement Certificati qualificati - Documenti di riconoscimento consentiti" Adeguamento normativo
5	28/12/2023	Intero documento: revisione annuale §1.6.1 Aggiunto riferimento a standard ETSI 319 411-1 Aggiunto riferimento a Determinazione AgID 147/2019 § 3.1.1 Deroga a RFC 5280 per la lunghezza di alcuni campi del subjectDN §4.9 Inserita informazioni sulla conservazione dello stato di revoca a seguito della scadenza del certificate di root. §4.9.3 Integrati riferimenti per certificati short-term § 5.1.6 Aggiornamento tecnologico dei supporti di Memorizzazione §5.7.3 Precisazioni su compromissioni delle chiavi §5.8 Inserita informazioni sulla conservazione dello stato di revoca in caso di cessazione della CA.

	§6.1.7 Modifica paragrafo con specifiche su utilizzo della chiave di CA (§6.1.7.1) e utilizzo della chiave del Titolare (§6.1.7.2) §9.17 Aggiornamento orari di erogazione servizi

9.12.2 Procedure di revisione

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le revisioni sono approvate dal Responsabile dei Servizi di Certificazione.

9.12.3 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del TSP (indirizzo: https://id.infocamere.it/digital-id/firma-digitale/manuali.html);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;
- in formato elettronico può essere richiesto alle Registration Authority.

In caso di variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative), si prevede un aggiornamento e verifica del Manuale Operativo, che segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda e conforme allo standard ISO 9001:2015. Tali modifiche saranno opportunamente notificate agli utenti in concomitanza della pubblicazione della nuova versione sul sito web https://id.infocamere.it.

9.12.4 Casi nei quali l'OID deve cambiare

n/a

9.13 Risoluzione delle controversie

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

9.14 Foro competente

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta InfoCamere S.C.p.A. e relative all'utilizzo del servizio di certificazione, alle modalità operative e all'applicazione delle disposizioni del presente Manuale sarà competente esclusivamente il Foro indicato nelle Condizioni Generali - Servizi di Certificazione pubblicate sul sito https://id.infocamere.it

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] 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 (divenuto pienamente applicabile il 25 maggio 2018) e Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii
[4] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori e relative normative nazionali di recepimento.
[5] Determinazione AgID n°189/2017.
[6] Determinazione AgID n°121/2019 (sostituisce deliberazione CNIPA 45/2009) rettificata dalla determinazione AgID n°147/2019.
[7] Allegato al Manuale Operativo / Certificate Policy e Certificate Practice Statement Certificati qualificati - Documenti di riconoscimento consentiti (IC-DOC-TSP)

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza[2], nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].

9.16 Disposizioni varie

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

9.17 Altre disposizioni

Gli orari di erogazione del servizio sono (salvo accordi contrattuali differenti):

Servizio	Orario
Accesso all'archivio pubblico dei certificati	Dalle 0:00 alle 24:00

[2] Disponibili sul sito https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata.

Servizio	Orario
(comprende i certificati e le CRL).	7 giorni su 7 (disponibilità minima 99%)
Revoca e sospensione dei certificati.	Dalle 0:00 alle 24:00 7 giorni su 7 (disponibilità minima 99%)
Altre attività: registrazione, generazione, pubblicazione[3].	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi
Rinnovo[4]	Dalle 00:00 alle 24:00 7 giorni su 7, attraverso il sito web id.infocamere.it
Richiesta e/o verifica di marca temporale.	24hx7gg (disponibilità minima 99%)
Assistenza – Call Center	Dal lunedì al venerdì dalle 08:30 alle 18:30 Esclusi i giorni festivi

[3] L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono scegliere diversi orari di sportello. In ogni caso InfoCamere garantisce l'erogazione del proprio servizio negli orari sopra riportati.

[4] Il servizio potrà non essere disponibile nella fascia oraria indicata per fermi di manutenzione o per cause di forza maggiore.

Appendice A

Certificato di root CA

```
 0 1911: SEQUENCE {
 4 1375:   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  169:     SEQUENCE {
34   11:       SET {
36    9:         SEQUENCE {
38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
43    2:           PrintableString 'IT'
     :         }
     :       }
47   28:       SET {
49   26:         SEQUENCE {
51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
56   19:           UTF8String 'InfoCamere S.C.p.A.'
     :         }
     :       }
77   41:       SET {
79   39:         SEQUENCE {
81    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
86   32:           UTF8String 'Qualified Trust Service Provider'
     :         }
     :       }
120  26:       SET {
122  24:         SEQUENCE {
124   3:           OBJECT IDENTIFIER '2 5 4 97'
129  17:           UTF8String 'VATIT-02313821007'
     :         }
     :       }
148  53:       SET {
150  51:         SEQUENCE {
152   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
157  44:           UTF8String
     :             'InfoCamere Qualified Electronic Signature CA'
     :         }
     :       }
     :     }
203  30:     SEQUENCE {
205  13:       UTCTime 04/12/2019 09:49:37 GMT
```

```
220  13:     UTCTime 04/12/2035 10:49:37 GMT
     :     }
235  169:   SEQUENCE {
238  11:    SET {
240  9:     SEQUENCE {
242  3:       OBJECT IDENTIFIER countryName (2 5 4 6)
247  2:       PrintableString 'IT'
     :     }
     :    }
251  28:    SET {
253  26:     SEQUENCE {
255  3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
260  19:      UTF8String 'InfoCamere S.C.p.A.'
     :     }
     :    }
281  41:    SET {
283  39:     SEQUENCE {
285  3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
290  32:      UTF8String 'Qualified Trust Service Provider'
     :     }
     :    }
324  26:    SET {
326  24:     SEQUENCE {
328  3:       OBJECT IDENTIFIER '2 5 4 97'
333  17:      UTF8String 'VATIT-02313821007'
     :     }
     :    }
352  53:    SET {
354  51:     SEQUENCE {
356  3:       OBJECT IDENTIFIER commonName (2 5 4 3)
361  44:      UTF8String
     :       'InfoCamere Qualified Electronic Signature CA'
     :     }
     :    }
     :   }
407  546:  SEQUENCE {
411  13:   SEQUENCE {
413  9:    OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
424  0:    NULL
     :    }
426  527:  BIT STRING, encapsulates {
431  522:   SEQUENCE {
435  513:    INTEGER
     :       00 89 29 F7 97 71 EE 30 F9 CD DB 12 6C 21 AB 97
     :       A0 90 C8 B3 45 1E CA 25 0F D0 A6 34 03 3B 7F E0
     :       2D 8C AB DD E4 01 AE CB 23 FF F8 A7 70 05 ED CF
     :       F7 DB 1C ED 2F 53 86 23 93 33 31 A9 57 BC 1F 7E
     :       C3 CD B3 3F 8F D1 FD 9A 85 5C 25 23 93 81 66 E9
     :       6E CF 9C 37 DB AD 5B A9 8F 98 D3 AD 15 DC 3F DF
     :       5A 4A 0C E1 5F D0 AC 90 F9 EA 03 B7 B5 AD 9D 3F
     :       01 94 22 1C 7E DE 6A 5E 3C 7D 4E 34 4E 13 1E CC
     :         [ Another 385 bytes skipped ]
952  3:      INTEGER 65537
```

```
    :        }
    :      }
    :    }
 957 422:   [3] {
 961 418:     SEQUENCE {
 965  15:       SEQUENCE {
 967   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 972   1:         BOOLEAN TRUE
 975   5:         OCTET STRING, encapsulates {
 977   3:           SEQUENCE {
 979   1:             BOOLEAN TRUE
    :           }
    :         }
    :       }
 982 253:       SEQUENCE {
 985   3:         OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
 990 245:         OCTET STRING, encapsulates {
 993 242:           SEQUENCE {
 996 239:             SEQUENCE {
 999 236:               [0] {
1002 233:                 [0] {
1005  41:                   [6]
    :                   'http://crl.ca.infocamere.it/ca/qc/ARL.crl'
1048 187:                   [6]
    :                   'ldap://ldap.ca.infocamere.it/cn%3DInfoCamere%20Q'
    :                   'ualified%20Electronic%20Signature%20CA,ou%3DQual'
    :                   'ified%20Trust%20Service%20Provider,o%3DInfoCamer'
    :                   'e%20S.C.p.A.,c%3DIT?authorityRevocationList'
    :                 }
    :               }
    :             }
    :           }
    :         }
    :       }
1238  96:       SEQUENCE {
1240   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
1245  89:         OCTET STRING, encapsulates {
1247  87:           SEQUENCE {
1249  85:             SEQUENCE {
1251   4:               OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
1257  77:               SEQUENCE {
1259  75:                 SEQUENCE {
1261   8:                   OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1271  63:                   IA5String
    :                   'https://id.infocamere.it/digital-id/firma-digita'
    :                   'le/manuali.html'
    :                 }
    :               }
    :             }
    :           }
    :         }
    :       }
1336  14:       SEQUENCE {
```

```
1338   3:        OBJECT IDENTIFIER keyUsage (2 5 29 15)
1343   1:        BOOLEAN TRUE
1346   4:        OCTET STRING, encapsulates {
1348   2:          BIT STRING 1 unused bit
       :           '1100000'B
       :         }
       :       }
1352  29:      SEQUENCE {
1354   3:        OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1359  22:        OCTET STRING, encapsulates {
1361  20:          OCTET STRING
       :           7A 80 68 6D D3 FC 79 62 D4 DD 6D CB C2 A3 EC 2B
       :           CD EA FE C1
       :         }
       :       }
       :     }
       :   }
       : }
1383  13:  SEQUENCE {
1385   9:    OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1396   0:    NULL
       :   }
1398 513:  BIT STRING
       :   1C FF D2 BF E4 D1 7D 47 98 8B E5 B9 98 96 C9 E3
       :   BD BF 43 4D D8 A9 74 8D 8B D9 EB 15 97 6E DB 5B
       :   41 DA 0C 18 2C 6F 7E 32 41 DD 49 6B 82 87 91 84
       :   62 CA 7B 30 21 54 56 A9 05 84 14 80 A2 4F 91 F6
       :   26 92 BD 1B 35 42 F2 3D CC EE 20 BD 8E 2D 4C C3
       :   8E A6 9D E0 A5 34 67 DF A5 CC A3 96 4F C6 B6 41
       :   F6 82 0D 85 08 60 78 76 78 2D ED 99 BC 74 05 A7
       :   E9 58 A9 A0 85 C4 D6 B5 76 9F D1 CF 8D E3 1E 13
       :         [ Another 384 bytes skipped ]
       : }
```

Formato delle CRL e OCSP

Estensione	Valore
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCamere
thisUpdate	Data in formato UTC
nextUpdate	Data della prossima CRL In format
Revoked Certificates List	Lista dei certificati revocati, con numero di serie e data di revoca/sospensione
Issuer's Signature	Firma della CA

Valori ed estensioni per CRL e OCSP

Le CRL hanno le seguenti estensioni:

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

La richiesta OCSP contiene i seguenti campi:

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

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	Stato della risposta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificato firmatario della risposta OCSP.
Produced at	Data in formato GeneralizedTime di quando è stata generate la risposta OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash del distinguishName dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente
Serial Number	Numero di serie del certificato
thisUpdate	La data di verifica dello stato del certificato in formato GeneralizedTime
nextUpdate	Data in cui lo stato del certificato potrebbe essere aggiornato
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

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

Appendice B

Strumenti e modalità per l'apposizione e la verifica della firma digitale

InfoCamere mette a disposizione un prodotto (denominato "Firma4NG") gratuitamente scaricabile dai Titolari e dagli Utenti dal sito https://id.infocamere.it per consentire:

- di firmare digitalmente documenti a tutti i Soggetti in possesso di un certificato emesso da InfoCamere;
- la verifica della firma apposta a documenti firmati digitalmente secondo i formati definiti dagli atti di implementazione del Regolamento.

Gli ambienti in cui Firma4NG opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto e le istruzioni di utilizzo, sono reperibili all'indirizzo web sopra indicato. La possibilità di visualizzare il file dipende dalla disponibilità sulla stazione di lavoro dell'utente di un adeguato software di visualizzazione. InfoCamere può mettere a disposizione, a pagamento e secondo gli accordi commerciali tempo per tempo stabiliti con le RA, i Richiedenti, i Soggetti o gli Utenti, ulteriori prodotti o servizi di firma e/o di verifica della firma. I documenti elettronici sottoscritti con certificati emessi da InfoCamere possono essere verificati anche attraverso altri strumenti, in grado di interpretare i formati di firma previsti. Tali strumenti sono fuori dalla responsabilità di InfoCamere.

Avvertenza

Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 25 comma 2 del Regolamento [1], ossia non può considerarsi equivalente rispetto a una firma autografa. È cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.