Manuale Operativo

Certificate Policy
Certificate Practice Statement

CODICE DOCUMENTO	ICERT-INDI-MO*
VERSIONE	4.11
DATA	15/05/2024

***** dalla versione 4.0, i documenti ICERT-INDI-MO e ICERT-INDI-MO-ENT sono confluiti in questo documento

INFOCERT
TINEXTA GROUP

SOMMARIO

1 INTRODUZIONE 8
1.1 Quadro generale 8
1.2 Nome ed identificativo del documento 8
1.3 Partecipanti e responsabilità 12
1.3.1 Certification Authority – Autorità di certificazione 12
1.3.2 Registration Authority – Ufficio di Registrazione (RA) 12
1.3.3 Soggetto 13
1.3.4 Utente 13
1.3.5 Richiedente 13
1.3.6 Autorità 14
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 15
1.5.1 Contatti 15
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 23
2 PUBBLICAZIONE E ARCHIVIAZIONE 27
2.1 Archiviazione 27
2.2 Pubblicazione delle informazioni sulla certificazione 27
2.2.1 Pubblicazione del Manuale Operativo 27
2.2.2 Pubblicazione dei certificati 27
2.2.3 Pubblicazione delle liste di revoca e sospensione 27
2.3 Periodo o frequenza di pubblicazione 28
2.3.1 Frequenza di pubblicazione del Manuale Operativo 28
2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione 28
2.4 Controllo degli accessi agli archivi pubblici 28
3 IDENTIFICAZIONE E AUTENTICAZIONE 29
3.1 Denominazione 29
3.1.1 Tipi di nomi 29
3.1.2 Necessità che il nome abbia un significato 29
3.1.3 Anonimato e pseudonimia dei richiedenti 29
3.1.4 Regole di interpretazione dei tipi di nomi 29
3.1.5 Univocità dei nomi 30
3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati 31
3.2 Convalida iniziale dell'identità 31
3.2.1 Metodo per dimostrare il possesso della chiave privata 31
3.2.2 Autenticazione dell'identità delle organizzazioni 31
3.2.3 Autenticazione della persona fisica 32
3.2.4 Informazioni del Soggetto o del Richiedente non verificate 40
3.2.5 Validazione dell'autorità 40
3.3 Identificazione e autenticazione nel caso di rinnovo o riemissione con nuove chiavi ... 41
3.3.1 Identificazione e autenticazione di un Soggetto nel caso di riemissione con nuove chiavi 41

InfoCert S.p.A. – all rights reserved

3.3.2 Identificazione e autenticazione di un Soggetto nel caso di riemissione con nuove chiavi dopo la revoca 41
3.3.3 Identificazione e autenticazione di un Soggetto per il rinnovo dei certificati 41
3.4 Identificazione e autenticazione per le richieste di revoca o sospensione 42
3.4.1 Richiesta da parte del Soggetto 42
3.4.2 Richiesta da parte del Richiedente 43
4 OPERATIVITÁ 43
4.1 Richiesta del certificato 43
4.1.1 Chi può richiedere il certificato 43
4.1.2 Processo di registrazione e responsabilità 43
4.2 Elaborazione della richiesta 44
4.2.1 Esecuzione delle funzioni di identificazione e autenticazione 44
4.2.2 Approvazione o rifiuto della richiesta del certificato 47
4.2.3 Tempo massimo per l'elaborazione della richiesta del certificato 47
4.3 Emissione del certificato 47
4.3.1 Azioni della CA durante l'emissione del certificato 47
4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato 49
4.3.3 Attivazione 49
4.4 Accettazione del certificato 49
4.4.1 Comportamenti concludenti di accettazione del certificato 49
4.4.2 Pubblicazione del certificato da parte della Certification Authority 49
4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato 50
4.5 Uso della coppia di chiavi e del certificato 50
4.5.1 Uso della chiave privata e del certificato da parte del Soggetto 50
4.5.2 Uso della chiave pubblica e del certificato da parte degli Utenti Finali 50
4.5.3 Limiti d'uso e di valore 51
4.6 Rinnovo del certificato 52
4.6.1 Motivi per il rinnovo 52
4.6.2 Chi può richiedere il rinnovo 53
4.6.3 Elaborazione della richiesta di rinnovo del certificato 53
4.7 Riemissione con nuove chiavi 53
4.7.1 Motivi per la riemissione con nuove chiavi 53
4.7.2 Chi può richiedere la riemissione con nuove chiavi 53
4.7.3 Elaborazione della richiesta di riemissione con nuove chiavi 53
4.8 Modifica del certificato 54
4.9 Revoca e sospensione del certificato 54
4.9.1 Motivi per la revoca 54
4.9.2 Chi può richiedere la revoca 55
4.9.3 Procedure per richiedere la revoca 55
4.9.4 Periodo di grazia della richiesta di revoca 56
4.9.5 Tempo massimo di elaborazione della richiesta di revoca 57
4.9.6 Requisiti per la verifica della revoca 57
4.9.7 Frequenza di pubblicazione della CRL 57
4.9.8 Latenza massima della CRL 57
4.9.9 Servizi online di verifica dello stato di revoca del certificato 58
4.9.10 Requisiti servizi online di verifica 58
4.9.11 Altre forme di revoca 58
4.9.12 Requisiti specifici rekey in caso di compromissione 58
4.9.13 Motivi per la sospensione 58
4.9.14 Chi può richiedere la sospensione 59

InfoCert S.p.A. – all rights reserved

4.9.15 Procedure per richiedere la sospensione 59
4.9.16 Limiti al periodo di sospensione 61
4.10 Servizi riguardanti lo stato del certificato 61
4.10.1 Caratteristiche operative 61
4.10.2 Disponibilità del servizio 61
4.10.3 Caratteristiche opzionali 62
4.11 Disdetta dai servizi della CA 62
4.12 Deposito presso terzi e recovery della chiave 62
5 MISURE DI SICUREZZA E CONTROLLI 63
5.1 Sicurezza fisica 63
5.1.1 Posizione e costruzione della struttura 63
5.1.2 Accesso fisico 64
5.1.3 Impianto elettrico e di climatizzazione 65
5.1.4 Prevenzione e protezione contro gli allagamenti 65
5.1.5 Prevenzione e protezione contro gli incendi 66
5.1.6 Supporti di memorizzazione 66
5.1.7 Smaltimento dei rifiuti 66
5.1.8 Off-site backup 66
5.2 Controlli procedurali 67
5.2.1 Ruoli chiave 67
5.3 Controllo del personale 67
5.3.1 Qualifiche, esperienze e autorizzazioni richieste 67
5.3.2 Procedure di controllo delle esperienze pregresse 67
5.3.3 Requisiti di formazione 67
5.3.4 Frequenza di aggiornamento della formazione 68
5.3.5 Frequenza nella rotazione dei turni di lavoro 68
5.3.6 Sanzioni per azioni non autorizzate 68
5.3.7 Controlli sul personale non dipendente 68
5.3.8 Documentazione che il personale deve fornire 68
5.4 Gestione del giornale di controllo 69
5.4.1 Tipi di eventi memorizzati 69
5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo 69
5.4.3 Periodo di conservazione del giornale di controllo 69
5.4.4 Protezione del giornale di controllo 69
5.4.5 Procedure di backup del giornale di controllo 70
5.4.6 Sistema di memorizzazione del giornale di controllo 70
5.4.7 Notifica in caso di identificazione di vulnerabilità 70
5.4.8 Valutazioni di vulnerabilità 70
5.5 Archiviazione dei verbali 70
5.5.1 Tipi di verbali archiviati 70
5.5.2 Protezione dei verbali 70
5.5.3 Procedure di backup dei verbali 70
5.5.4 Requisiti per la marcatura temporale dei verbali 71
5.5.5 Sistema di memorizzazione degli archivi 71
5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi 71
5.6 Sostituzione della chiave privata della CA 71
5.7 Compromissione della chiave privata della CA e disaster recovery 71
5.7.1 Procedure per la gestione degli incidenti 71
5.7.2 Corruzione delle macchine, del software o dei dati 72
5.7.3 Procedure in caso di compromissione della chiave privata della CA 72

InfoCert S.p.A. – all rights reserved

5.7.4 Erogazione dei servizi di CA in caso di disastri ... 72
5.8 Cessazione del servizio della CA o della RA ... 72
6 CONTROLLI DI SICUREZZA TECNOLOGICA ... 74
6.1 Installazione e generazione della coppia di chiavi di certificazione ... 74
6.1.1 Generazione della coppia di chiavi del Soggetto ... 74
6.1.2 Consegna della chiave privata al Richiedente ... 75
6.1.3 Consegna della chiave pubblica alla CA ... 75
6.1.4 Consegna della chiave pubblica agli utenti ... 75
6.1.5 Algoritmo e lunghezza delle chiavi ... 75
6.1.6 Controlli di qualità e generazione della chiave pubblica ... 76
6.1.7 Scopo di utilizzo della chiave ... 76
6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico ... 76
6.2.1 Controlli e standard del modulo crittografico ... 76
6.2.2 Controllo di più persone della chiave privata di CA ... 77
6.2.3 Deposito presso terzi della chiave privata di CA ... 77
6.2.4 Backup della chiave privata di CA ... 77
6.2.5 Archiviazione della chiave privata di CA ... 77
6.2.6 Trasferimento della chiave privata da un modulo o su un modulo crittografico ... 77
6.2.7 Memorizzazione della chiave privata su modulo crittografico ... 77
6.2.8 Metodo di attivazione della chiave privata ... 77
6.2.9 Metodo di disattivazione della chiave privata ... 78
6.2.10 Metodo per distruggere la chiave privata della CA ... 78
6.2.11 Classificazione dei moduli crittografici ... 78
6.3 Altri aspetti della gestione delle chiavi ... 78
6.3.1 Archiviazione della chiave pubblica ... 78
6.3.2 Periodo di validità del certificato e della coppia di chiavi ... 78
6.4 Dati di attivazione della chiave privata ... 78
6.5 Controlli sulla sicurezza informatica ... 79
6.5.1 Requisiti di sicurezza specifici dei computer ... 79
6.6 Operatività sui sistemi di controllo ... 79
6.7 Controlli di sicurezza della rete ... 79
6.8 Sistema di validazione temporale ... 80
7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP ... 81
7.1 Formato del certificato ... 81
7.1.1 Numero di versione ... 81
7.1.2 Estensioni del certificato ... 81
7.1.3 OID dell'algoritmo di firma ... 81
7.1.4 Forme di nomi ... 81
7.1.5 Vincoli ai nomi ... 82
7.1.6 OID del certificato ... 82
7.2 Formato della CRL ... 82
7.2.1 Numero di versione ... 82
7.2.2 Estensioni della CRL ... 82
7.3 Formato dell'OCSP ... 82
7.3.1 Numero di versione ... 82
7.3.2 Estensioni dell'OCSP ... 82
8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ ... 83
8.1 Frequenza o circostanze per la valutazione di conformità ... 83
8.2 Identità e qualifiche di chi effettua il controllo ... 83
8.3 Rapporti tra InfoCert e CAB ... 83

InfoCert S.p.A. – all rights reserved

8.4 Aspetti oggetto di valutazione ... 83
8.5 Azioni in caso di non conformità ... 84
9 ALTRI ASPETTI LEGALI E DI BUSINESS ... 85
9.1 Tariffe ... 85
9.1.1 Tariffe per il rilascio, il rinnovo e la riemissione con nuove chiavi dei certificati ... 85
9.1.2 Tariffe per l'accesso ai certificati ... 85
9.1.3 Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati ... 85
9.1.4 Tariffe per altri servizi ... 85
9.1.5 Politiche per il rimborso ... 85
9.2 Responsabilità finanziaria ... 86
9.2.1 Copertura assicurativa ... 86
9.2.2 Altre attività ... 86
9.2.3 Garanzia o copertura assicurativa per i soggetti finali ... 86
9.3 Confidenzialità delle informazioni di business ... 86
9.3.1 Ambito di applicazione delle informazioni confidenziali ... 86
9.3.2 Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali ... 86
9.3.3 Responsabilità di protezione delle informazioni confidenziali ... 86
9.4 Privacy ... 86
9.4.1 Programma sulla privacy ... 87
9.4.2 Dati che sono trattati come personali ... 87
9.4.3 Dati non considerati come personali ... 87
9.4.4 Titolare del trattamento dei dati personali ... 87
9.4.5 Informativa privacy e consenso al trattamento dei dati personali ... 87
9.4.6 Divulgazione dei dati a seguito di richiesta da parte dell'Autorità ... 88
9.4.7 Altri motivi di divulgazione ... 88
9.5 Proprietà intellettuale ... 88
9.6 Rappresentanza e garanzie ... 88
9.7 Limitazioni di garanzia ... 89
9.8 Limitazioni di responsabilità ... 89
9.9 Indennizzi ... 90
9.10 Termine e risoluzione ... 90
9.10.1 Termine ... 90
9.10.2 Risoluzione ... 90
9.10.3 Effetti della risoluzione ... 91
9.10.4 Canali di comunicazione ufficiali ... 91
9.10.5 Revisione del Manuale Operativo ... 91
9.10.6 Storia delle revisioni ... 91
9.10.7 Procedure di revisione ... 101
9.10.8 Periodo e meccanismo di notifica ... 101
9.10.9 Casi nei quali l'OID deve cambiare ... 101
9.11 Risoluzione delle controversie ... 101
9.12 Foro competente ... 101
9.13 Legge applicabile ... 102
9.14 Disposizioni varie ... 103
9.15 Altre disposizioni ... 103
APPENDICE A ... 104
Electronic Signature Qualified Root "InfoCert Firma Qualificata 2" ... 104
Electronic Signature Qualified Root "InfoCert Qualified Electronic Signature CA 3" ... 107

InfoCert S.p.A. – all rights reserved

Electronic Signature Qualified Root "InfoCert Qualified Electronic Signature CA 4" 110
Electronic Signature Qualified Root "InfoCert Qualified Electronic Signature EC CA 4" 114
Estensioni del certificato 117
Estensioni QCStatement per QSealC PSD2 121
Formato delle CRL e OCSP 121
Valori ed estensioni per CRL e OCSP 122
APPENDICE B 125
Strumenti e modalità per l'apposizione e la verifica della firma digitale 125
APPENDICE C 126
Certificato qualificato del Cittadino Spagnolo persona fisica su QSCD emesso dalla root CA "InfoCert Qualified Electronic Signature CA 4" 126
AVVERTENZA 128

InfoCert S.p.A. – all rights reserved

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 è il Manuale Operativo del **Prestatore di Servizi Fiduciari InfoCert** (*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 ed emissione del certificato qualificato, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, e in generale descrive 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 chiavi 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.

Il presente Manuale Operativo contiene altresì le politiche e le pratiche seguite da InfoCert S.p.A. (nel prosieguo, anche semplicemente, "**InfoCert**") nel processo di controllo delle richieste, identificazione dei richiedenti ed emissione dei certificati per autenticazione siti web di cui all'art 34 Regolamento Delegato (UE) 2018/389 [12], di attuazione della Direttiva (UE) 2015/2366 (PSD2) [11], in conformità con i requisiti definiti dallo standard ETSI TS 119 495 (referenziati nel seguito come "Certificati PSD2").

1.2 Nome ed identificativo del documento

Questo documento è denominato "Prestatore di Servizi Fiduciari InfoCert – Manuale Operativo" ed è caratterizzato dal codice documento: ICERT-INDI-MO. La versione e

InfoCert S.p.A. – all rights reserved

il livello di rilascio sono identificabili nell'intestazione di ogni pagina.
La versione 4.0 del presente documento si pone in continuità e sostituisce i previgenti Manuali Operativi denominati:

- ICERT-INDI-MO, versione 3.5 del 30/11/2018 per l'emissione di certificati qualificati a persona fisica e giuridica anche a mezzo di un sistema CMS
- ICERT-INDI-MO-ENT, versione 3.5 del 30/11/2018, per l'emissione di certificati qualificati a persona fisica di tipo LongTerm e OneShot

descrivendo in un unico documento le politiche e procedure per la gestione dei certificati qualificati secondo il regolamento eIDAS [1].
Al documento sono associati gli Object Identifier (OID), descritti in seguito, che sono referenziati nell'estensione CertificatePolicy dei certificati, secondo l'utilizzo cui gli stessi sono destinati. Il significato degli OID è il seguente:

L'*object identifier* (OID) che identifica InfoCert è 1.3.76.36.
Le policy per certificati qualificati sono:

Descrizione	**OID**
Manuale-operativo-certificato qualificato emesso a persona fisica	1.3.76.36.1.1.48.1 conforme alla policy QCP-n 0.4.0.194112.1.0
Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo (SSCD)	1.3.76.36.1.1.48.2 conforme alla policy QCP-n 0.4.0.194112.1.0
Manuale-operativo-certificato qualificato emesso a persona giuridica anche su dispositivo (SSCD) Disponibile anche per PSD2 (QSealC)	1.3.76.36.1.1.47 conforme alla policy QCP-l 0.4.0.194112.1.1

Le policy per certificati qualificati su dispositivo qualificato sono:

InfoCert S.p.A. – all rights reserved

Descrizione	OID
Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo qualificato (QSCD)	1.3.76.36.1.1.1/1.3.76.36.1.1.61 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 qualificato (QSCD)	1.3.76.36.1.1.2/1.3.76.36.1.1.62 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 (QSCD)	1.3.76.36.1.1.22/1.3.76.36.1.1.63 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona fisica attraverso un sistema CMS su dispositivo qualificato (QSCD)	1.3.76.36.1.1.32/1.3.76.36.1.1.66 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato emesso a persona giuridica su dispositivo qualificato (QSCD) Disponibile anche per PSD2 (QSealC)	1.3.76.36.1.1.46 conforme alla policy QCP-l-qscd 0.4.0.194112.1.3
Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo qualificato (QSCD) di tipo LongTerm	1.3.76.36.1.1.35/1.3.76.36.1.1.65 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 (QSCD) di tipo OneShot	1.3.76.36.1.1.34/1.3.76.36.1.1.64 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2
Manuale-operativo-certificato qualificato del “Cittadino Spagnolo” emesso a persona fisica e chiavi su dispositivo qualificato (QSCD)	1.3.76.36.1.1.10.16.1.1.1 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2

Di seguito vengono elencate le policy per certificati qualificati su dispositivo qualificato definiti con key usage settings di tipo B o F come indicato al par. 4.3.2 dello standard ETSI EN 319 412-2. Poiché combinare il bit di non ripudio con i bit di

InfoCert S.p.A. – all rights reserved

digital signature e key encipherment può avere impatti di sicurezza, l'utilizzo di questi OID è limitato e ogni richiesta viene valutata singolarmente.

Descrizione	OID
Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo qualificato (QSCD) e key usage settings Type B o F	1.3.76.36.1.1.61.1 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 (QSCD) e key usage settings Type B o F	1.3.76.36.1.1.63.1 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 (QSCD) di tipo LongTerm e key usage settings Type B o F	1.3.76.36.1.1.65.1 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 (QSCD) di tipo OneShot e key usage settings Type B o F	1.3.76.36.1.1.64.1 conforme alla policy QCP-n-qscd 0.4.0.194112.1.2

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel § 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 della Determinazione AgID n. 121/2019 con le rettifiche della successiva Determinazione AgID n. 147/2019 [13], dal 5 luglio 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 sul sito Web del Prestatore di Servizi Fiduciari all'indirizzo: https://www.firma.infocert.it ovvero sul sito istituzionale https://www.infocert.it, 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.

InfoCert S.p.A. – all rights reserved

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.
InfoCert è la Certification Authority (di seguito, anche semplicemente **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: InfoCert – Società per azioni - Società soggetta a direzione e coordinamento di Tinexta S.p.A.
Sede legale: Piazza Sallustio n.9, 00187, Roma (RM)
Sedi operative:

- Via Marco e Marcelliano n.45, 00147, Roma (RM)
- Via Fernanda Wittgens n. 2, 20123 Milano (MI)
- Piazza Luigi da Porto n. 3, 35131 Padova (PD)

Rappresentante legale: Danilo Cattaneo, in qualità di Amministratore Delegato
N. di telefono: 06 836691
Codice fiscale e n. Iscrizione Registro Imprese: 07945211006
Numero REA: RM - 1064345
N. partita IVA: 07945211006
Sito web: https://www.infocert.it

1.3.2 Registration Authority – Ufficio di Registrazione (RA)

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

- l'identificazione del Soggetto o del Richiedente,
- la registrazione dei dati del Soggetto,
- l'inoltro dei dati del Soggetto ai sistemi della CA,
- la raccolta della richiesta del certificato qualificato,
- la distribuzione e/o inizializzazione del dispositivo sicuro di firma, ove presente,
- l'attivazione della procedura di certificazione della chiave pubblica,

InfoCert S.p.A. – all rights reserved

- 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; la CA verifica la rispondenza delle procedure utilizzate a quanto stabilito dal presente Manuale.

1.3.2.1 Incaricato alla registrazione o Registration Authority Officer

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

1.3.3 Soggetto

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 ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

1.3.5 Richiedente

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

- può coincidere con il Soggetto se questi è una persona fisica,

InfoCert S.p.A. – all rights reserved

- può essere la persona fisica che ha i poteri di richiedere un certificato per una persona giuridica,
- può essere la persona giuridica che richiede il certificato per persone fisiche a essa legate da rapporti commerciali ovvero nell'ambito di organizzazioni,
- può essere il genitore o chi ne fa le veci in caso di soggetto minorenne sopra i 14 anni compiuti.

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.

1.3.6.3 Autorità nazionale competente (NCA)

In ambito PSD2[11], l'autorità nazionale di vigilanza degli intermediari finanziari è l'organismo responsabile dell'autorizzazione dei PSP di ciascun stato membro. Se l'autorizzazione è concessa, l'Autorità nazionale competente (di seguito, anche semplicemente, "**NCA**") emette un numero di autorizzazione e pubblica tali informazioni nei propri registri pubblici.

1.3.6.4 Autorità bancaria europea (EBA)

L'autorità bancaria europea (di seguito, anche semplicemente, "**EBA**"), opera per assicurare un livello di regolamentazione e di vigilanza uniforme nel settore

InfoCert S.p.A. – all rights reserved

bancario europeo. In ambito PSD2[11], vigila e si fa garante della trasparenza dell'operato dei prestatori di servizi di pagamento (PSP) autorizzati dalle NCA competenti per ciascuno stato membro. Ha in carico lo sviluppo e la gestione del "Registro elettronico centrale", nel quale ogni NCA deve pubblicare l'elenco di nomi e le informazioni riferite ai soggetti autorizzati.

1.4 Uso del certificato

1.4.1 Usi consentiti

I certificati emessi dalla CA InfoCert, secondo le modalità indicate dal presente Manuale Operativo, sono Certificati Qualificati ai sensi del CAD e del Regolamento eIDAS.
Il certificato emesso dalla CA sarà usato per verificare la firma qualificata o il sigillo elettronico del Soggetto cui il certificato appartiene.
La CA InfoCert mette a disposizione per la verifica delle firme alcuni prodotti disponibili sul sito InfoCert. 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

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Domande, reclami, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte ai seguenti recapiti:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telefono: 06 836691
Call Center: consultare il link https://help.infocert.it/contatti/ per maggiori dettagli
Web: https://www.firma.infocert.it, https://www.infocert.it
e-mail: firma.digitale@legalmail.it

InfoCert S.p.A. – all rights reserved

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

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

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

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale seguono le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.
Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

1.6 Definizioni e acronimi

1.6.1 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal Regolamento eIDAS [1] e dal CAD [2] si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Termine	Definizione
Autocertificazione	È la dichiarazione, rivolta alla CA, effettuata personalmente dal soggetto che risulterà Soggetto del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità con assunzione delle responsabilità stabilite per legge.

InfoCert S.p.A. – all rights reserved

Termine	Definizione
Conformity Assessment Body (Organismo di valutazione della conformità) (CAB)	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.
Conformity Assessment Report (Relazione di valutazione della conformità) (CAR)	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]).
Card Management System (CMS)	Strumento di autenticazione, identificazione, raccolta e conservazione dei dati relativi ai Soggetti o ai Richiedenti.
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 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]).
Certificato qualificato di sigillo elettronico per PSD2 (QSealC PSD2)	QSealC di cui all'art 34 Regolamento Delegato (UE) 2018/389 [12], di attuazione della Direttiva (UE) 2015/2366 (PSD2) [11], in conformità con i requisiti definiti dallo standard ETSI TS 119 495 (referenziati nel seguito come "QSealC PSD2")

InfoCert S.p.A. – all rights reserved

Termine	Definizione
Certificato LongTerm	Particolare certificato qualificato di firma elettronica qualificata per procedura remota il cui utilizzo è limitato esclusivamente a un dominio informatico per il quale è stato emesso.
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 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.
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]).
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]).
Cliente	Soggetto con cui InfoCert ha formalizzato un contratto di fornitura di servizi dietro pagamento di corrispettivo
Codice di emergenza (ERC)	Codice di sicurezza consegnato al Soggetto per inoltrare la richiesta di sospensione di un certificato sui portali del TSP.
Convalida	Il processo di verifica e conferma della validità di una firma elettronica (cfr eIDAS [1]).
Dati di convalida	Dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1]).

InfoCert S.p.A. – all rights reserved

Termine	Definizione
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 (SSCD secure system creation device)	Un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica qualificata 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]).
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1]).
Dominio informatico	Si identifica con le applicazioni per mezzo delle quali il certificato qualificato è rilasciato al Soggetto e all'interno delle quali il Soggetto può utilizzare il certificato per la sottoscrizione di documenti informatici. Le applicazioni possono essere gestite direttamente dal Certificatore ovvero dal Richiedente e possono contenere altresì disposizioni particolari aggiuntive a seconda della procedura di identificazione adottata per il rilascio del certificato qualificato.
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.

InfoCert S.p.A. – all rights reserved

Termine	Definizione
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]).
Giornale di controllo	Consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [9].
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]).

InfoCert S.p.A. – all rights reserved

Termine	Definizione
Lista dei certificati revocati o sospesi (Certificate Revocation List – CRL)	È una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel registro pubblico.
Manuale operativo (certificate practice statement - CPS)	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.
One Time Password (OTP)	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]).

InfoCert S.p.A. – all rights reserved

Termine	Definizione
Prestatore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr eIDAS [1]).
Prodotto	Un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari (cfr eIDAS [1]).
Pubblico ufficiale	Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.
Registro pubblico [Directory]	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	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: creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure creazione, verifica e convalida di certificati di autenticazione di siti web; o conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1]).
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1]).

InfoCert S.p.A. – all rights reserved

Termine	Definizione
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	Definizione
AgID	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
CA	Certification Authority
CAB	Conformity Assessment Body – Organismo di

InfoCert S.p.A. – all rights reserved

Acronimo	Definizione
	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
CMS	Card Management System
CNS – TS-CNS	Carta Nazionale dei Servizi Tessera Sanitaria – Carta Nazionale dei Servizi
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguish Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority
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 o Registration Authority Officer
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

InfoCert S.p.A. – all rights reserved

Acronimo	Definizione
	1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
IUT	Identificativo Univoco del Titolare: è un codice associato al Soggetto che lo identifica univocamente presso la CA; il Soggetto ha codici diversi per ogni certificato in suo possesso
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati
LoA	Level of Assurance
NCA	National Competent Authority
NTR Code	National Trade Register Code
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
OTP	OneTime Password
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal 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
PSD2	Payment Services Directive 2
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,

InfoCert S.p.A. – all rights reserved

Acronimo	Definizione
	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
UUID	Universally unique identifier
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

InfoCert S.p.A. – all rights reserved

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Archiviazione

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

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del Manuale Operativo

Il presente Manuale Operativo, 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 a InfoCert l'apposito modulo (disponibile sul sito www.firma.infocert.it), compilato e firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione. L'invio deve avvenire via e-mail indirizzata a richiesta.pubblicazione@cert.legalmail.it seguendo la procedura descritta sul sito stesso. Tale possibilità non è prevista per i certificati LongTerm e 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 "CRL Distribution Points" del certificato. Tale accesso può essere effettuato tramite i software messi a disposizione dalla CA e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP e/o HTTP.
La CA potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

InfoCert S.p.A. – all rights reserved

2.3 Periodo o frequenza di pubblicazione

2.3.1 Frequenza di pubblicazione del Manuale Operativo

Il Manuale Operativo viene pubblicato ove indicato al par. 1.5.1 con frequenza variabile quando avvengono dei cambiamenti. Se i cambiamenti sono importanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il Manuale Operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

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

2.4 Controllo degli accessi agli archivi pubblici

Le informazioni relative ai certificati pubblicati, alle CRL 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.

InfoCert S.p.A. – all rights reserved

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 negli standard ETSI EN 319 412 dall'1 al 5.
Tuttavia, gli standard ETSI EN 319 412-2 par. 4.2.4 e 319 412-3 par. 4.2.1 consentono sia per certificati a persona fisica sia a persona giuridica una lunghezza maggiore di quanto stabilito nella specifica RFC 5280 per i campi *givenName, surname, commonName.*
In accordo a tale deroga sono stati individuati i seguenti limiti massimi: *givenName* e *surname* 40 caratteri, *commonName* 81 caratteri.

In base al contesto si seguono le indicazioni della determinazione AgID 147/2019 [13] o di altri Paesi purché non in contrasto con il Regolamento eIDAS [1].

3.1.2 Necessità che il nome abbia un significato

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

3.1.3 Anonimato e pseudonimia dei richiedenti

Solo in caso di identificazione secondo la modalità 1_LiveID (vedi § 3.2.3.1) è facoltà del Soggetto richiedere alla CA che il certificato riporti uno pseudonimo in luogo dei propri dati reali. Tale possibilità non è prevista per i certificati LongTerm e OneShot. Poiché il certificato è qualificato, la CA conserverà le informazioni relative alla reale identità della persona per almeno venti (20) anni dalla scadenza del certificato stesso, fino a un massimo di 23 (ventitre) anni dalla data di emissione.

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert si attiene allo standard X500.

InfoCert S.p.A. – all rights reserved

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.
In assenza di TIN o Codice Fiscale, nel certificato potrà essere indicato:

- un codice identificativo tratto da un documento di identità valido, utilizzato nella procedura di riconoscimento. Il formato è quello previsto dallo std ETSI 319 412-1,
- un identificativo univoco determinato dalla CA. Il formato utilizzato in questo caso è UUID (Identificativo Univoco Universale) di tipo 4 descritto in RFC4122,
- un identificativo univoco come descritto in EIDAS eID profile nell'ambito di EIDAS cooperation network. Il documento di riferimento è "eIDAS SAML AttributeProfileVersion" ver 1.2. (https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+eID+Profile),
- un altro identificativo univoco attribuito nell'ambito dell'ordine, associazione o più genericamente nell'organizzazione di appartenenza.

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

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)
- LEI (Legal Entity Identifier).

Nel caso di persone giuridiche italiane, il codice identificativo utilizza 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 [13].

InfoCert S.p.A. – all rights reserved

Nel caso di utilizzo del codice LEI, nell'estensione country code del certificato deve essere indicato "XG" in conformità allo standard ETSI 319 412-1.
Si precisa inoltre che sono possibili eccezioni nel caso di emissione di certificati afferenti a particolari circuiti.

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.
Nel commonName di un certificato di sigillo è consentito utilizzare un marchio registrato.
La CA non fa verifiche sull'utilizzo di marchi, pertanto il Soggetto e il Richiedente si assumono la piena responsabilità in merito all'utilizzo di marchi registrati all'interno del certificato.
La CA può inoltre rifiutarsi di generare o può richiedere di revocare un certificato coinvolto in una disputa.

3.2 Convalida iniziale dell'identità

Questo capitolo descrive le procedure usate per l'identificazione del 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

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

3.2.2 Autenticazione dell'identità delle organizzazioni

La richiesta di certificato per persona giuridica deve essere effettuata da una persona fisica identificata in una delle modalità descritte al § 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.
La persona giuridica può essere un prestatore di servizi di pagamento (PSP) soggetto a direttiva PSD2.

InfoCert S.p.A. – all rights reserved

La CA verifica il nome dell'organizzazione e la sua esistenza tramite l'uso di basi dati governative o di terze parti o tramite comunicazioni dirette con l'ente che sovrintende la creazione e il riconoscimento di un'entità legale nel paese in cui è stabilita.

In particolare,

- per le imprese private italiane o straniere le verifiche si basano sulle visure estratte dal registro imprese in cui la legal entity è registrata; l'accesso ai dati dei registri imprese avviene tramite il servizio fornito da Innolva per la consultazione del Registro delle Imprese tramite il link: https://areainterna.assicom.com/area_interna/ oppure tramite il portale https://e-justice.europa.eu/content_business_registers_in_member_states-106- en.do;
- per le pubbliche amministrazioni italiane, le verifiche avvengono tramite il portale IPA https://indicepa.gov.it/ipa-portale/.

3.2.3 Autenticazione della persona fisica

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

InfoCert S.p.A. – all rights reserved

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
1 LiveID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione • Pubblico Ufficiale • Datore di Lavoro per la identificazione dei propri dipendenti, collaboratori, agenti	n/a
2 AMLID	• Soggetti destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive normative comunitarie di esecuzione	n/a
3 SignID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	Utilizzo di una firma elettronica qualificata emessa da un Prestatore di Servizi Fiduciari Qualificato
4 AutID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	Utilizzo di un mezzo di identificazione elettronica preesistente

InfoCert S.p.A. – all rights reserved

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
5.1 VideoID assistito (attended)	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	n/a
5.2 VideoID non assistito (unattended)	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	n/a
5.3 VideoID semiautomatico (SelfQ)	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	n/a
6 eDocId	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	Utilizzo di un mezzo di identificazione elettronica preesistente
7 ContoID	• Certification Authority (CA)	Strong Customer Authentication per l'accesso al conto bancario

Nell'Addendum [14] 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.

3.2.3.1 Riconoscimento effettuato secondo la modalità 1 -LiveID

La modalità di identificazione **LiveID** prevede un incontro di persona tra il Soggetto e uno dei soggetti abilitati a eseguire il riconoscimento.
Il Soggetto esibisce all'incaricato della CA, che è appositamente formato, uno o più documenti d'identificazione in originale e in corso di validità, ricompresi nella lista dei documenti accettati pubblicati sulla sezione Documentazione del sito della CA https://www.firma.infocert.it ovvero sul sito istituzionale https://www.infocert.it[2].
Per garantire l'univocità del Soggetto e del relativo nome, questi deve essere in possesso anche del codice identificativo univoco di cui al § 3.1.5 Il soggetto abilitato

[2] La lista dei documenti di riconoscimento accettati è redatta dalla CA previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte della Autorità Emittenti. La lista è notificata a AgID e aggiornata ad ogni modifica.

InfoCert S.p.A. – all rights reserved

ad eseguire il riconoscimento, nel caso riscontri incongruenze rispetto a quanto dichiarato dal richiedente, può richiedere l'esibizione di documentazione che comprovi il possesso di tale identificativo univoco.
Le Registration Authority operanti all'estero, o che comunque identificano Soggetti residenti all'estero, possono essere autorizzate da InfoCert ad accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, ricompresi nella lista dei documenti accettati pubblicata sulla sezione Documentazione del sito della CA https://www.firma.infocert.it ovvero sul sito istituzionale https://www.infocert.it.
L'identificazione può essere eseguita anche da parte di un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività. Il Soggetto compila la richiesta di Certificazione e la sottoscrive di fronte ad un Pubblico Ufficiale, facendo autenticare la propria firma ai sensi delle normative vigenti. La richiesta è poi presentata alla CA ad uno degli Uffici di Registrazione convenzionati.
Una particolare identificazione LiveID viene eseguita, previa verifica delle procedure operative di identificazione e di autenticazione, dal datore di lavoro, ai fini della stipula del contratto di lavoro, e viene definita Employee ID. Analogamente, è considerata valida in conformità alla seguente modalità di riconoscimento, l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia, previa verifica delle procedure operative di identificazione e di autenticazione.
Questa modalità di identificazione prevede il conferimento da parte della CA di un mandato con rappresentanza al datore di lavoro, che agisce quindi da RA[3]. I Certificati emessi secondo questa modalità di identificazione possono essere utilizzati solamente per le finalità di lavoro per le quali sono rilasciati, e contengono uno specifico limite d'uso.
I dati di registrazione per la modalità di identificazione LiveID sono conservati dalla CA in formato analogico o in formato elettronico.

3.2.3.2 Riconoscimento effettuato secondo la modalità 2 - AMLID

Nella **modalità 2 - AMLID** la CA si avvale dell'identificazione eseguita da uno dei soggetti destinatari degli obblighi di Identificazione e Adeguata Verifica, ai sensi delle normative tempo per tempo vigenti, di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive ulteriori normative comunitarie di aggiornamento e esecuzione.

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

InfoCert S.p.A. – all rights reserved

Con specifico riferimento al contesto italiano, i dati utilizzati per il riconoscimento sono rilasciati dal Soggetto ai sensi del D.Lgs. 231/2007 e s.m.i., a norma del quale i clienti sono tenuti a fornire - sotto la propria responsabilità - tutte le informazioni necessarie e aggiornate per consentire ai Soggetti destinatari degli Obblighi di adempiere agli obblighi di identificazione della clientela.
Questa modalità di identificazione prevede il conferimento, da parte della CA, di un mandato con rappresentanza al soggetto destinatario degli obblighi, che agisce quindi da RA. I dati identificativi del Soggetto raccolti all'atto del riconoscimento sono conservati dalla CA di norma in modalità elettronica e possono essere conservati anche in modalità analogica.

3.2.3.3 Riconoscimento effettuato secondo la modalità 3 - SignID

Nella **modalità 3 SignID** la CA InfoCert si basa sul riconoscimento già effettuato da una CA che emette certificati qualificati (QTSP)***.*** Il Soggetto è già in possesso di un certificato qualificato ancora in corso di validità, che utilizza nei confronti di InfoCert. I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.
La richiesta di un certificato può essere fatta in modalità SignID solamente se il certificato qualificato utilizzato per firmare tale richiesta non è stato emesso a sua volta nella modalità SignID.

3.2.3.4 Riconoscimento effettuato secondo la modalità 4 - AUTID

Nella **modalità 4 AutID** la CA si basa su un mezzo di identificazione elettronica preesistente in corso di validità, ovvero non scaduto, né revocato o sospeso:

- 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;
- Emesso da una autorità pubblica o un soggetto privato, ulteriormente confermato dal Titolare mediante l'autenticazione sul proprio conto di pagamento eseguita mediante Strong Customer Authentication (SCA) da un Payment Service Provider (PSP), in conformità alla Direttiva UE 2015/2366 (PSD2).

Con specifico riferimento al quadro di interoperabilità definito dall'articolo 12 del

InfoCert S.p.A. – all rights reserved

Regolamento eIDAS, il messaggio restituito dal nodo EIDAS a fronte dell'utilizzo di un sistema di identificazione nazionale notificato, di livello almeno significativo, si considera sufficiente per l'emissione di un certificato qualificato. Il messaggio è di tipo SAML come previsto dalle specifiche CEF (Connecting Europe Facility) nell'ambito del programma CEF eID[4], ed è inviato alla CA dal soggetto gestore del nodo nazionale ovvero da uno dei soggetti autorizzati ad avvalersi del nodo stesso. La CA verifica l'integrità del messaggio SAML ricevuto e considera identificato il soggetto sulla base dei dati contenuti nel messaggio stesso.

Con specifico riferimento al contesto italiano, sono mezzi di identificazione elettronica la tessera CNS (Carta nazionale dei Servizi) o TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi), la CIE (Carta di Identità Elettronica), il permesso di soggiorno elettronico e le identità rilasciate nel contesto del sistema SPID.

I mezzi di identificazione elettronica utilizzabili dalla CA e dalle RA sono elencati nella lista pubblicata sul sito della CA e notificata a AgID.
InfoCert valuterà della possibilità di avvalersi di identificazioni effettuate da soggetti in possesso di un una certificazione rilasciata da un CAB che attesti che la modalità di identificazione utilizzata è conforme all'art. 24 lett. d) eIDAS.

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

3.2.3.5 Riconoscimento effettuato secondo la modalità 5 - VideoID

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

La modalità di identificazione 5 - VideoID può configurarsi alternativamente:

5.1 Con presenza contestuale dell'Incaricato alla Registrazione e del Soggetto o Richiedente all'interno della medesima sessione audiovideo (VideoID assistito); 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 pubblicata sul sito della CA[5].

[4] Tali specifiche sono al seguente link https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile
[5] La lista dei documenti di riconoscimento accettati è redatta dalla CA previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte della Autorità Emittenti. La lista è notificata a

InfoCert S.p.A. – all rights reserved

5.2 Senza la presenza contestuale dell'Incaricato alla Registrazione e del Soggetto o Richiedente all'interno della sessione audiovideo. In questa configurazione il Soggetto effettua in autonomia la sessione audio-video e, inoltre, esegue come azione di conferma della sua identità l'invio di una transazione bancaria da un conto corrente ad esso intestato o cointestato, indicando nella causale lo specifico codice di correlazione fornito dalla CA o dalla RA. In una fase di backoffice successiva, l'Incaricato alla Registrazione visiona l'audio-video, la coincidenza tra l'intestazione del bonifico e i dati del Soggetto e la correttezza del codice di correlazione e, in caso di controlli superati, procede alla validazione dell'identità (VideoID non assistito).

5.3 Senza la presenza contestuale dell'Incaricato alla Registrazione e del Soggetto o Richiedente all'interno della sessione audiovideo, con strumenti automatizzati di validazione (SelfQ). In questa configurazione, il Soggetto è guidato in una procedura di raccolta di copia del documento d'identità e in una procedura automatica di ripresa del suo volto (c.d. "video-selfie"), durante la quale compie alcune azioni casuali di rafforzamento. La CA applica tecnologie di validazione documentale per accertare l'autenticità del documento di identità presentato, ne estrae i dati e la foto e ne riscontra la reale appartenenza al Soggetto utilizzando una o più tecnologie biometriche di confronto tra la foto estratta e il video-selfie raccolto. Qualora l'indice di compatibilità (c.d. "scoring") non raggiunga valori sufficienti, un Incaricato alla Registrazione provvede a eseguire una successiva fase di verifica dell'identità in backoffice.

Inoltre, la video identificazione potrà avvenire secondo le modalità operative e di processo approvate da un diverso Organismo di Vigilanza notificato alla Commissione in conformità all'articolo 17 del Regolamento eIDAS in conformità con la rispettiva normativa nazionale implementazione dell'articolo 24 del Regolamento, purché queste non comportino la violazione della normativa italiana[6].

Le RA operanti all'estero, o che comunque identificano Soggetti residenti all'estero, possono essere autorizzate da InfoCert ad accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte delle Autorità Emittenti, nonché specifica formazione[7].
È facoltà dell'Incaricato alla Registrazione 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

AgID e aggiornata ad ogni modifica. Per ragioni di sicurezza e procedure antifrode, il tipo di documenti accettati da questa modalità è limitato ai documenti di identità maggiormente diffusi
[6] Tali casi saranno comunicati all'Autorità di Vigilanza.
[7] Tali casi saranno comunicati all'Autorità di Vigilanza.

InfoCert S.p.A. – all rights reserved

formato elettronico, sono conservati in forma protetta.

3.2.3.6 Riconoscimento effettuato secondo la modalità 6 - eDocID

Nella modalità 6 eDocID, il Soggetto è in possesso di un device collegato a Internet, munito di webcam e lettore di prossimità, e presenta per l'identificazione un documento di identità leggibile meccanicamente utilizzabile per l'identificazione biometrica[8].
Inquadrando il documento con la fotocamera e avvicinandolo al lettore di prossimità, il Soggetto consente l'accesso alla memoria elettronica del chip, da cui sono estratti i dati identificativi e la foto ivi contenuti; il Soggetto è inoltre guidato in una procedura automatica di ripresa del suo volto (c.d. "video-selfie"), durante la quale compie alcune azioni casuali di rafforzamento, seguendo le istruzioni della procedura predisposte dalla CA.
La CA verifica l'autenticità della firma tecnica presente su dati e foto estratte dal documento di identità e ne riscontra la reale appartenenza al Soggetto utilizzando una o più tecnologie biometriche di confronto tra la foto estratta e il video-selfie raccolto. Qualora l'indice di compatibilità (c.d. "scoring") non raggiunga valori sufficienti, un Incaricato alla Registrazione provvede a eseguire una successiva fase di verifica dell'identità in backoffice.
I dati di registrazione, costituiti da file video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

3.2.3.7 Riconoscimento effettuato secondo la modalità 7 - ContoID

Nella modalità 7 ContoID, il Soggetto è in possesso di un device collegato a Internet munito di webcam e presenta per l'identificazione un documento di identità in corso di validità.
Inquadrando il documento con la fotocamera, il Soggetto è guidato in una procedura di raccolta di copia del documento d'identità per consentirne l'estrazione dei relativi dati identificativi e della foto. Il Soggetto è inoltre guidato in una procedura automatica di ripresa del suo volto (c.d. "video-selfie"), durante la quale compie alcune azioni casuali di rafforzamento, seguendo le istruzioni della procedura predisposta dalla CA.
La CA verifica la reale appartenenza del documento al Soggetto utilizzando una o più tecnologie biometriche di confronto tra la foto estratta e il video-selfie raccolto; è inoltre verificato che i dati di intestazione del conto corrispondano con i dati del Soggetto stesso.
Il Soggetto conferma i propri dati mediante l'autenticazione sul proprio conto di

[8] Si tratta di documenti conformi alle norme ICAO con MRZ, o comunque aventi caratteristiche di sicurezza paragonabili

InfoCert S.p.A. – all rights reserved

pagamento eseguita mediante Strong Customer Authentication (SCA) da un Payment Service Provider (PSP), in conformità alla Direttiva UE 2015/2366 (PSD2).
I dati di registrazione, costituiti da file 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, direttamente o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di informazioni relative a:

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

Il certificato con il **Ruolo** è conforme a quanto indicato nella Determina AgID 147/2019 [13].
Il Soggetto deve produrre la dichiarazione idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo mediante Autocertificazione[9]. La CA non assume alcuna responsabilità, salvo i casi di dolo o colpa, in merito all'inserimento nel certificato delle informazioni autocertificate dal Soggetto.
La ragione sociale o la denominazione e il codice identificativo dell'**Organizzazione** saranno invece riportate nel certificato se essa ha autorizzato il rilascio del certificato al Soggetto, anche senza l'esplicita indicazione di un ruolo. In tale ipotesi la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Soggetto. La richiesta di certificati con l'indicazione del Ruolo e/o dell'Organizzazione può provenire solo da organizzazioni che hanno una forma giuridica definita.

3.2.5 Validazione dell'autorità

La CA ovvero la RA verificano le informazioni richieste definite nei § 3.2.2 , 3.2.3 e 3.2.4, per l'identificazione e validano la richiesta.
La CA ovvero la RA, dove previsto o necessario, può avvalersi di banche dati pubbliche per la validazione delle informazioni fornite dal richiedente.

In caso di richiesta QSealC PSD2, la CA ovvero RA verifica gli attributi specifici forniti dal soggetto Richiedente (numero di autorizzazione, nome e stato della NCA, ruolo

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

InfoCert S.p.A. – all rights reserved

del PSP) utilizzando le informazioni autentiche rese disponibili da EBA all'interno del proprio registro centrale o, eventualmente, nei registri resi disponibili dalle NCA di ciascuno stato membro.
Se la NCA nazionale ha fornito delle regole per la convalida di tali attributi, il TSP applica le regole indicate.

3.3 Identificazione e autenticazione nel caso di rinnovo o riemissione con nuove chiavi

Questo paragrafo descrive le procedure usate per l'autenticazione e identificazione del Soggetto quando richiede di rinnovare il proprio certificato o quando richiede una riemissione di certificato con nuove e diverse chiavi crittografiche.

3.3.1 Identificazione e autenticazione di un Soggetto nel caso di riemissione con nuove chiavi

La riemissione di certificato con nuove chiavi può avvenire prima della scadenza del certificato cioè quando "valido fino al" (not after) è successivo alla data della richiesta; utilizzando gli strumenti messi a disposizione dalla CA, il Soggetto può fare la richiesta sottoscritta con la chiave privata corrispondente alla chiave pubblica contenuta nel certificato già in suo possesso. In questo caso possiamo anche chiamarlo **rinnovo con ri-certificazione di nuove chiavi.**
Il soggetto può richiedere una riemissione del certificato anche dopo la scadenza del precedente certificato cioè quando "valido fino al" (not after) è precedente alla data della richiesta. Il certificatore può avvalersi del riconoscimento del Soggetto fatto precedentemente e del legame sicuro stabilito in precedenza tra le credenziali del Soggetto e il suo riconoscimento. Tale legame è garantito dal doppio fattore di autenticazione che in fase di riconoscimento è stato associato al Soggetto stesso.
Il riconoscimento viene mantenuto valido per un massimo di quattro anni e solo se i documenti di identità del richiedente o altri attributi legati all'identità del Soggetto nel frattempo non sono scaduti.
Il certificatore può decidere, talora riscontri problematiche legate alla sicurezza delle informazioni o problematiche legate a frodi, di invalidare il riconoscimento anche prima dei quattro anni.

3.3.2 Identificazione e autenticazione di un Soggetto nel caso di riemissione con nuove chiavi dopo la revoca

n/a

3.3.3 Identificazione e autenticazione di un Soggetto per il rinnovo

InfoCert S.p.A. – all rights reserved

dei certificati

Questo paragrafo descrive le procedure usate per l'autenticazione e identificazione del Soggetto nel caso di rinnovo del certificato qualificato di firma, mantenendo le stesse chiavi crittografiche.
Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (validity) con gli attributi "valido dal" (not before) e "valido fino al" (not after). Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.
Il Soggetto può, tuttavia, rinnovarlo, prima della sua scadenza, utilizzando gli strumenti messi a disposizione dalla CA, che presentano una richiesta di rinnovo che viene sottoscritta con la chiave privata corrispondente alla chiave pubblica contenuta nel certificato da rinnovare. Dopo la revoca o la scadenza del certificato non è possibile eseguire il rinnovo del certificato, diventando quindi necessaria una nuova emissione.

3.4 Identificazione e autenticazione per le richieste di revoca o sospensione

La revoca o sospensione del certificato può avvenire su richiesta autenticata 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 (vd § 4.9).
La richiesta di sospensione può essere fatta attraverso un form Internet, in tal caso il Soggetto si autentica fornendo il codice di emergenza consegnato al momento dell'emissione del certificato, oppure con un altro sistema di autenticazione descritto nella documentazione contrattuale consegnata all'atto della registrazione.
Il soggetto in possesso di una firma remota può richiedere la revoca anche utilizzando la sua area privata a cui accede attraverso un sistema di autenticazione a due fattori (§ 4.2.2)

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

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

InfoCert S.p.A. – all rights reserved

3.4.2 Richiesta da parte del Richiedente

Il Richiedente o un terzo interessato che richiede la revoca o sospensione del certificato del Soggetto si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dalla CA. La richiesta dovrà essere inoltrata con le modalità indicate ai § 4.9.3 o 4.9.15.2. La CA si riserva di individuare ulteriori modalità di inoltro della richiesta, di revoca o sospensione del Richiedente in apposite convenzioni da stipulare con lo stesso.

4 OPERATIVITÁ

4.1 Richiesta del certificato

4.1.1 Chi può richiedere il certificato

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

- Il Soggetto
  - rivolgendosi direttamente alla CA al sito www.firma.infocert.it o www.infocert.it, ovvero
  - rivolgendosi a una Registration Authority
- Il Richiedente per conto del Soggetto
  - rivolgendosi direttamente alla CA mediante il sito www.firma.infocert.it o www.infocert.it o stipulando un accordo commerciale con la CA
  - rivolgendosi a una Registration Authority
  - sottoscrivendo il mandato con rappresentanza con la CA e diventando Registration Authority all'interno di un dominio informatico.

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

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

4.1.2 Processo di registrazione e responsabilità

Il processo di registrazione comprende: la richiesta da parte del Soggetto, la generazione della coppia di chiavi, la richiesta di certificazione della chiave pubblica e la firma dei contratti, non necessariamente in quest'ordine.

InfoCert S.p.A. – all rights reserved

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 idonea procura, che richiede il certificato qualificato per conto della persona giuridica medesima;
- 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.

Nel caso il Soggetto sia una persona giuridica, quando le chiavi sono generate in un dispositivo del Soggetto, il Richiedente deve inviare anche la richiesta in formato PKCS#10 firmata dal richiedente stesso.

4.2 Elaborazione della richiesta

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

- prendere visione della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel § 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 Esecuzione delle funzioni di identificazione e autenticazione

4.2.1.1 Persona fisica

Per la richiesta di un certificato qualificato di sottoscrizione il Soggetto o il

InfoCert S.p.A. – all rights reserved

Richiedente che richiede il certificato della persona fisica deve fornire obbligatoriamente le seguenti informazioni:

- Cognome e Nome;
- Data e luogo di nascita;
- Codice TIN (codice fiscale nel contesto italiano) o, in sua assenza, analogo codice identificativo quale il numero del documento di identità; nei casi in cui la normativa del Paese non permette l'utilizzo pubblico di queste informazioni, InfoCert non le inserirà nel certificato.
- Estremi del documento di riconoscimento presentato per l'identificazione, quali ad esempio tipo o numero.;
- Almeno un dato di contatto per l'invio delle comunicazioni dalla CA al Soggetto, tra
    - Indirizzo di residenza
    - Indirizzo e-mail;
- numero di telefonia mobile, per contatto di emergenza e per la trasmissione dell'OTP ove fosse questa la tecnologia OTP adottata.

L'indirizzo e-mail e il numero di cellulare forniti alla RA, devono essere esistenti e identificare univocamente il Soggetto. L'indirizzo e-mail sarà usato per eventuali comunicazioni dalla CA e per l'invio dei codici di emergenza (ERC) e gli avvisi di scadenza. Questa considerazione non è applicabile nei casi di certificati LongTerm e OneShot.

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;
- Indirizzo e-mail per l'invio delle comunicazioni dalla CA al Richiedente;

InfoCert S.p.A. – all rights reserved

- Nome del Soggetto persona giuridica;
- VAT code ovvero NTR (partita IVA o numero di Registro Imprese per i Soggetti italiani,).

Nel caso in cui la persona giuridica volesse certificare le proprie coppie di chiavi, il richiedente deve fornire anche il file in formato PKCS#10 della richiesta firmata dal Richiedente.
Le informazioni fornite sono memorizzate negli archivi della CA (fase di registrazione) e saranno la base per la generazione del certificato qualificato.

In caso di richiesta di QSealC PSD2, il soggetto (PSP), individuato nel legale rappresentante o persona fisica dotata di procura, **deve fornire le seguenti ulteriori informazioni:**

- numero di autorizzazione che identifica univocamente il prestatore di servizio di pagamento (PSP);
- ruolo/i del prestatore di servizio di pagamento (PSP);
- nome e stato dell'autorità nazionale competente (NCA) che ha autorizzato prestatore di servizio di pagamento (PSP) e ha rilasciato il numero di autorizzazioni.

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 alla attivazione del dispositivo di firma o della procedura di firma, se remota, sia alla eventuale richiesta di sospensione del certificato (codice ERC o codice analogo, se previsto dal contratto). Tali codici di sicurezza sono consegnati in modalità elettronica e trasmessi all'interno di file cifrati.
L'emissione dei codici di sicurezza consegnati in busta cieca è in dismissione. Potrà essere utilizzata solo in casi rari in cui non sarà possibile l'utilizzo della modalità elettronica.
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 attraverso un sistema di autenticazione erogato dalla RA, avente livello di sicurezza almeno significativo o elevato previa analisi delle caratteristiche del sistema stesso, nell'ambito del perimetro di certificazione del dispositivo sicuro di firma. In questi casi il sistema di autenticazione può essere usato anche per l'eventuale richiesta di sospensione e revoca del certificato.

InfoCert S.p.A. – all rights reserved

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 ovvero 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

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 RA.
La coppia di chiavi crittografiche viene generata sull'HSM sito presso la sede del QTSP; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica attraverso un canale sicuro.
La Certification Authority, verificata la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che viene memorizzato sull'HSM stesso.

InfoCert S.p.A. – all rights reserved

4.3.1.3 Emissione del certificato attraverso un sistema di Card Management System

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

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.

4.3.1.4 Emissione del certificato a persona giuridica

La coppia di chiavi crittografiche viene generata dalla RA direttamente sull'HSM; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10, che è firmata digitalmente con il certificato 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.
Nel caso in cui la coppia di chiavi sia generata nel dispositivo HSM del Soggetto, questi dovrà inviare il PKCS#10 firmato e la Certification Authority, verificata la validità della firma sul PKCS#10 e la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che viene memorizzato sull'HSM stesso.

4.3.1.5 Emissione certificato con finalità di test

A volte è necessario utilizzare certificati per eseguire qualche test in ambiente di produzione.
In questi casi, prima di procedure all'emissione del certificato è necessario procedere alla registrazione dei dati. Tale registrazione deve essere approvata dal Responsabile della CA.
Nei casi previsti, l'Ufficio di registrazione deve essere l'Ufficio utilizzato da InfoCert per le emissioni interne, oppure l'Ufficio utilizzato dalla procedura del Cliente oggetto di una sessione di test.
I dati utilizzati per la registrazione devono indicare inequivocabilmente nel Subject che si tratta di un certificato di test e non di un certificato effettivo.
Tale procedura non può essere utilizzata per test di carico o cicliche su registrazioni e emissioni.
Nel momento in cui non dovesse più servire (ad es terminata sessione specifica di

InfoCert S.p.A. – all rights reserved

test), il certificato deve essere Revocato d'ufficio.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

In caso di emissione su dispositivo crittografico il Soggetto (o il Richiedente) non ha bisogno di notifica poiché il certificato è presente nel dispositivo che ha ricevuto.
In caso di certificati LongTerm e OneShot, la CA notifica al Richiedente con una procedura automatizzata che il certificato del Soggetto è stato emesso. Il Richiedente provvede a informare il Soggetto secondo le forme e i modi previsti dal contratto.
Negli altri casi il Soggetto riceverà la notifica attraverso l'indirizzo e-mail che ha indicato al momento dell'iscrizione. Tale informazione può essere condivisa anche col Richiedente

4.3.3 Attivazione

4.3.3.1 Attivazione del dispositivo di firma (smartcard o token)

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

4.3.3.2 Attivazione del dispositivo di firma remota (HSM)

Il Soggetto ovvero il Richiedente per conto di un soggetto giuridico, autenticato ai portali della CA attraverso i codici di attivazione ricevuti in maniera riservata, sceglie il PIN di firma, quantità di sicurezza riservata la cui custodia e tutela è posta esclusivamente in capo al Soggetto stesso, che viene confermato con l'inserimento della OneTime Password ricevuta via SMS, ovvero generata sul token o la token-app associata al certificato.
In alcuni casi il certificato può essere emesso già attivo e utilizzabile.

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

InfoCert S.p.A. – all rights reserved

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 LongTerm e 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 conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo, se presente, ovvero dagli strumenti o i codici di autenticazione. Deve garantire la protezione della segretezza e la conservazione del codice di emergenza necessario alla sospensione del certificato, ove presente. 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.
Nel caso di dominio informatico chiuso, il certificato LongTerm e OneShot deve essere usato solamente per firmare documenti afferenti al rapporto specifico tra Richiedente e Soggetto.

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.

InfoCert S.p.A. – all rights reserved

4.5.3 Limiti d'uso e di valore

È possibile richiedere alla RA, presentando adeguata documentazione a supporto, l'inserimento nel certificato qualificato di sottoscrizione, dei seguenti limiti d'uso definiti da AgID:

- 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.
- L'utilizzo del certificato è limitato ai rapporti con (*indicare il soggetto*). The certificate may be used only for relations with the (*declare the subject*).

I certificati qualificati di sottoscrizione **per procedura automatica** contengono il limite d'uso definito da Agid:

Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.

I certificati emessi sulla base dell'**identificazione di tipo 4-AutID** attraverso il **nodo eIDAS** oppure sulla base dell'identificazione di tipo **eDocID** contengono l'OID 1.3.76.16.5 e il seguente limite d'uso:

- Certificate not usable to require SPID digital identity

I certificati emessi sulla base dell'**identificazione di tipo 4-AutID** utilizzando **identità digitali SPID** in ottemperanza all'avviso n° 17 del 24 gennaio 2019, contengono l'OID 1.3.76.16.5 e il seguente limite d'uso:

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

I certificati a persona giuridica con codice LEI emessi per PoC (Proof of Concepts) contengono il seguente limite d'uso:

- The use of the certificate is limited for sealing the documents used in the Proof of Concepts about the incorporation of the LEI codes in the electronic seal certificates.

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

InfoCert S.p.A. – all rights reserved

Per quanto riguarda i limiti d'uso previsti per la Pubbliche Amministrazioni Spagnole valgono le considerazioni riportate in Appendice C e i riferimenti normativi [17], [18], [19].

Limiti d'utilizzo per certificati LongTerm e OneShot

I certificati di tipo LongTerm possono essere limitati esclusivamente all'utilizzo nel dominio informatico specificato dal contratto, per la sottoscrizione dei documenti informatici resi disponibili al Soggetto dalla CA o dal Richiedente. In tal caso i documenti informatici possono essere inerenti a rapporti tra lo stesso Richiedente e il Soggetto.
Nel **certificato LongTerm**, quindi, viene riportato uno dei seguenti limiti d'uso:

- Il certificato è utilizzabile solo nei rapporti tra titolare e richiedente. The certificate can be used only in the relationships between the holder and the requestor (max 200 caratteri).
- Certificato per la sottoscrizione di prodotti e servizi resi disponibili da [Nome Soggetto]. Certificate to subscribe product and services made available by [Nome Soggetto] (max 200 caratteri).

Il **certificato OneShot** riporta 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.

Ferma restando la responsabilità della CA di cui al CAD (art.30), è responsabilità dell'Utente (colui che riceve il documento firmato) 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.

4.6 Rinnovo del certificato

4.6.1 Motivi per il rinnovo

Il rinnovo consente al Soggetto di ottenere un nuovo certificato a partire da un certificato in suo possesso prossimo alla scadenza. Per rinnovo si intende che il nuovo certificato conterrà gli stessi dati identificativi del Soggetto, la stessa chiave pubblica e una nuova data di scadenza. Per i certificati LongTerm e OneShot e per i certificati emessi a una persona giuridica non è previsto il rinnovo ma si procede ad un nuovo riconoscimento ed una nuova emissione.

InfoCert S.p.A. – all rights reserved

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 emissione precedente sono ancora valide; oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla richiesta di un nuovo certificato.
La procedura di rinnovo si applica esclusivamente a certificati emessi da InfoCert.

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 con nuove chiavi

4.7.1 Motivi per la riemissione con nuove chiavi

La riemissione del certificato con una nuova chiave (re-key) consente ad un Soggetto già identificato e in possesso di un certificato, di certificare una diversa coppia di chiavi, mantenendo gli stessi dati identificativi. La data di scadenza del nuovo certificato è definita contrattualmente.
Esempi, non esaustivi, possono essere la ri-certificazione di una nuova coppia di chiavi su dispositivo remoto in prossimità della scadenza del certificato o su un dispositivo in dismissione, o la sostituzione di chiavi crittografiche deboli con chiavi crittografiche generate con algoritmi più robusti.

La procedura si applica esclusivamente a certificati emessi da InfoCert.

4.7.2 Chi può richiedere la riemissione con nuove chiavi

La richiesta può essere fatta dal Soggetto o dal Richiedente prima della scadenza del certificato o successivamente, a patto che tutte le informazioni fornite all'atto della emissione precedente e le evidenze raccolte nella fase di riconoscimento siano ancora valide. Nel caso in cui il documento di identità non sia più valido il certificato non potrà essere riemesso.

4.7.3 Elaborazione della richiesta di riemissione con nuove chiavi

La riemissione con nuove chiavi viene eseguita attraverso un servizio messo disposizione dalla CA, nell'ambito dei rapporti commerciali e contrattuali definiti con il Soggetto e con la RA, dove presente.

InfoCert S.p.A. – all rights reserved

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 InfoCert 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.

InfoCert S.p.A. – all rights reserved

4.9.2 Chi può richiedere la revoca

La revoca del certificato può essere richiesta:

- dal Soggetto titolare del certificato;
- dal Richiedente o terzo interessato;
- d'ufficio dalla CA;
- dalla NCA, nel caso di richiesta di revoca di QSealC PSD2.

4.9.3 Procedure per richiedere la revoca

Di seguito vengono riportate le procedure attraverso le quali i legittimati della revoca possono richiederla.

Richiesta da parte del Soggetto: la richiesta di revoca può essere avanzata attraverso la sottoscrizione di un modulo presente sul sito InfoCert. Il modulo di cui sopra può essere consegnato alla RA o inviato direttamente alla CA per posta raccomandata, PEC, corredata da una fotocopia di un documento di identità in corso di validità. Inoltre, la CA o la RA possono mettere a disposizione ulteriori modalità per l'inoltro della richiesta di revoca, a condizione che queste prevedano una corretta identificazione del Soggetto. La CA o la RA ne danno adeguata comunicazione al Soggetto.

La CA o la RA verificano l'autenticità della richiesta, a seguito della quale procederanno alla revoca del certificato, dandone immediata notizia al Soggetto e, se presente, al Richiedente.

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. 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. Modalità aggiuntive per la richiesta di revoca da parte del Soggetto potranno essere specificate negli eventuali accordi tra il Soggetto e la CA.

Nel caso di richiesta di revoca per certificati LongTerm e OneShot, ad esclusione dei certificati short-term, il Soggetto può richiedere la revoca del certificato autenticandosi ai sistemi messi a disposizione dalla RA e/o dalla CA, mediante servizi applicativi, operando secondo le modalità descritte nella documentazione contrattuale. Per la definizione stessa del certificato short-term, non è prevista la richiesta di revoca da parte del Soggetto.

Richiesta da parte del Richiedente o terzo interessato: può richiedere la revoca

InfoCert S.p.A. – all rights reserved

del certificato del Soggetto con le stesse modalità con cui può richiederla il Soggetto purché opportunamente legittimato. Dovrà inoltre specificare i dati del Soggetto del certificato comunicati alla CA al momento dell'emissione del certificato.

La CA o la 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 Soggetto potranno essere specificate negli eventuali accordi tra il Soggetto e la CA o RA.

Nel caso di richiesta di revoca per certificati LongTerm e OneShot, ad esclusione dei certificati short-term, il Richiedente può richiedere la revoca del certificato del Soggetto autenticandosi ai sistemi messi a disposizione dalla CA, mediante servizi applicativi, operando secondo le modalità descritte nella documentazione contrattuale.
Per la definizione stessa del certificato short-term, non è prevista la richiesta di revoca da parte del Richiedente.

Revoca d'ufficio da parte della CA/RA: qualora se ne verifichi la necessità, la CA ha facoltà di revocare il certificato, comunicandolo preventivamente al Soggetto, fornendo il motivo della revoca, nonché la data e l'ora di decorrenza.

La CA/RA, 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. La CA/RA provvederà a comunicare l'avvenuta revoca anche al Richiedente.

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.

Richiesta della NCA: nel caso di richiesta di revoca di QSealC PSD2, la revoca può essere richiesta dalla NCA che ha rilasciato il numero di autorizzazione al prestatore di servizi di pagamento (PSP), presente nel certificato.

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

InfoCert S.p.A. – all rights reserved

la CRL corrente. Per non causare disservizi ad ogni parte coinvolta, questo periodo è più lungo del periodo di tempo di cui la CA ha bisogno per generare e pubblicare una nuova CRL. In questo modo la CRL corrente rimane valida almeno fino a quando non viene sostituita dalla nuova CRL.

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

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

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

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

4.9.8 Latenza massima della CRL

Una volta verificata l'autenticità della richiesta di revoca o sospensione, Il tempo di attesa tra l'inoltro alla CA e la sua realizzazione tramite pubblicazione della CRL è al massimo di un'ora.

InfoCert S.p.A. – all rights reserved

4.9.9 Servizi online di verifica dello stato di revoca del certificato

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

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.
Le informazioni sullo stato del certificato saranno rese disponibili fino alla scadenza del certificato di root CA.

4.9.10 Requisiti servizi online di verifica

Vd. appendice A

4.9.11 Altre forme di revoca

n/a

4.9.12 Requisiti specifici rekey in caso di compromissione

n/a

4.9.13 Motivi per la sospensione

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

1. sia 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 abbiano acquisito elementi di dubbio sulla validità del certificato ovvero sull'identità del Soggetto o del Richiedente (ad es., per sospetto o denunciato furto o frode di identità);
3. siano insorti dubbi sulla sicurezza del dispositivo di firma o del dispositivo OTP, qualora presente;
4. sia necessaria un'interruzione temporanea della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato, eventualmente specificandone la durata; alla scadenza di tale periodo, o alla richiesta di

InfoCert S.p.A. – all rights reserved

riattivazione del certificato, seguirà o una revoca definitiva oppure la ripresa di validità dello stesso.
In caso di sospetto furto di identità, la CA, senza preavviso, potrà procedere a una sospensione cautelativa.

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 CPS. Infine, il certificato può essere sospeso d'ufficio dalla CA.

4.9.15 Procedure per richiedere la sospensione

La sospensione del certificato è richiedibile nell'apposita sezione del sito della CA. La durata della sospensione viene scelta dal soggetto richiedente, se non specificata il certificato rimane sospeso fino a scadenza del certificato e poi revocato. La sospensione termina l'ultimo giorno del periodo di sospensione richiesto.
Per alcuni clienti, a fronte di accordi contrattuali specifici, viene messa a disposizione una funzione di riattivazione; in questo caso il certificato si può riattivare solo se non scaduto.

4.9.15.1 Sospensione richiesta dal Soggetto

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

utilizzando la funzione di sospensione disponibile nel sito web della CA o, nel caso di certificati di firma remota, tramite il portale MySign (strumento messo a disposizione da InfoCert per la gestione del certificato di firma remota), comunicando i dati richiesti e utilizzando il codice di emergenza fornito in sede di emissione del certificato, se noto.
utilizzando (ove disponibile) la funzione di sospensione con OTP disponibile nel sito Web indicato nella documentazione contrattuale fornita all'atto della Registrazione.
telefonando al Call Center della CA e fornendo le informazioni richieste In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una sospensione immediata del certificato per una durata di 10 (dieci) giorni solari in attesa della richiesta scritta del Soggetto; qualora la CA non riceva la richiesta sottoscritta entro il termine indicato, procede a riattivare il certificato.
tramite i canali di contatto della Registration Authority, la quale richiede i dati ed i documenti necessari, effettuando tutte le verifiche sull'identità del Soggetto; quindi,

InfoCert S.p.A. – all rights reserved

procede a richiedere la sospensione alla CA
utilizzando la funzione di sospensione disponibile sul sito WEB della RA di interfaccia verso i servizi CMS.

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

Qualora nel certificato oggetto della richiesta di sospensione sia presente l'indicazione dell'Organizzazione, la CA provvederà a comunicare l'avvenuta sospensione a tale soggetto.

La CA, qualora il contratto relativo al certificato oggetto della sospensione lo preveda, provvederà a comunicare l'avvenuta sospensione anche al Richiedente.
Per la definizione stessa del certificato short-term, non è prevista la richiesta di sospensione 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.

Nel caso di richiesta di sospensione per certificati LongTerm e OneShot, ad esclusione dei certificati short-term, il Richiedente può richiedere la sospensione del certificato del Soggetto autenticandosi ai sistemi messi a disposizione dalla CA, anche mediante servizi applicativi, operando secondo le modalità descritte nella documentazione contrattuale. Per la definizione stessa del certificato short-term, non è prevista la richiesta di sospensione 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

InfoCert S.p.A. – all rights reserved

e la data di termine. Queste ultime informazioni saranno in ogni caso comunicate al più presto al Soggetto.
La CA, qualora nel certificato oggetto della sospensione siano presenti informazioni relative al Ruolo del Soggetto, provvederà a comunicare l'avvenuta sospensione all'eventuale Terzo Interessato con cui siano operative le specifiche convenzioni. La CA, qualora nel certificato oggetto della sospensione sia presente l'indicazione dell'Organizzazione, provvederà a comunicare l'avvenuta sospensione a tale soggetto.
La CA, qualora il contratto relativo al certificato oggetto della sospensione lo preveda, provvederà a comunicare l'avvenuta sospensione anche al Richiedente.

4.9.16 Limiti al periodo di sospensione

La durata della sospensione viene scelta dal soggetto richiedente e non può essere superiore al periodo di validità del certificato. Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL). La riattivazione avviene nell'arco delle 24 ore successive alla data di termine della sospensione. Qualora il giorno di scadenza della sospensione coincida con il giorno di scadenza del certificato, la sospensione viene tramutata in revoca, con effetto dall'inizio della sospensione.
Ove previsto dal contratto, è possibile richiedere la riattivazione del certificato prima della data del termine di sospensione.
Nei casi in cui il certificato è stato sospeso attraverso un CMS è possibile utilizzare la funzione di riattivazione disponibile nel sito WEB di interfaccia verso i servizi CMS.

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.

InfoCert S.p.A. – all rights reserved

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

InfoCert S.p.A. – all rights reserved

5 MISURE DI SICUREZZA E CONTROLLI

Il TSP InfoCert 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 InfoCert è disponibile facendone richiesta alla casella PEC infocert@legalmail.it.
Le politiche di sicurezza in InfoCert 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 quand'anche 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 sito primario di erogazione InfoCert si trova a Padova. Il sito di Disaster Recovery è ubicato a Modena ed è connesso al Data Center sopra citato tramite un collegamento dedicato e ridondato su due circuiti diversi MPLS a 40 Gbit/s ciascuno upgradabile fino a 100 Gbit/s.

InfoCert S.p.A. – all rights reserved

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

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

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

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

5.1.2 Accesso fisico

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

InfoCert S.p.A. – all rights reserved

5.1.3 Impianto elettrico e di climatizzazione

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

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

L'infrastruttura preposta all'alimentazione include:

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

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

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

L'area tecnica è normalmente mantenuta fra 20° e 27° con un tasso di umidità relativo compreso fra il 30% ed il 60%. Gli impianti sono dotati di batterie condensanti con sistema di raccolta e scarico condensa sigillato e controllato da sonde antiallagamento. 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

InfoCert S.p.A. – all rights reserved

rispetto al livello della strada.

5.1.5 Prevenzione e protezione contro gli incendi

È presente nel Data Center un impianto di rilevazione fumi gestito da centrale analogica indirizzata NOTIFIER con sensori ottici posizionati in ambiente e nel controsoffitto e sensori a campionamento d'aria installati sottopavimento e nelle canalizzazioni dell'aria.
L'impianto di rilevazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici ARGON IG-01.
Nel caso di intervento contemporaneo di due rivelatori nella stessa zona, è comandata la scarica di estinguente nella zona interessata.
Per ogni compartimento antincendio è previsto un impianto di estinzione dedicato.
Sono inoltre presenti mezzi estinguenti portatili in conformità alle leggi e normative vigenti.

5.1.6 Supporti di memorizzazione

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp (FAS 8060). Per la parte SAN si è invece implementata un'infrastruttura per la parte data center basata su tecnologie Infinidat che comprendono n.2 enclosure InfiniBox di generazione F4000 e F6000; per la parte di CA l'infrastruttura si basa su tecnologia Pure Storage.

5.1.7 Smaltimento dei rifiuti

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

5.1.8 Off-site backup

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

InfoCert S.p.A. – all rights reserved

5.2 Controlli procedurali

5.2.1 Ruoli chiave

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

5.3 Controllo del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

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

5.3.2 Procedure di controllo delle esperienze pregresse

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con il responsabile della selezione e un successivo colloquio tecnico con il responsabile di Funzione/Struttura Organizzativa, volto a verificare le skill dichiarate dal candidato. Ulteriori strumenti di verifica sono esercitazioni e test.

5.3.3 Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, è previsto di affidare la gestione operativa del sistema a persone diverse, con compiti separati e ben definiti. Il personale addetto alla progettazione ed erogazione del servizio di certificazione è un dipendente InfoCert ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici, con caratteristiche di affidabilità e riservatezza. Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

InfoCert S.p.A. – all rights reserved

5.3.4 Frequenza di aggiornamento della formazione

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

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

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

5.3.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.
Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 (dieci) giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.
Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicendare nella reperibilità il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

5.3.6 Sanzioni per azioni non autorizzate

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

5.3.7 Controlli sul personale non dipendente

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

5.3.8 Documentazione che il personale deve fornire

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto in formato tessera

InfoCert S.p.A. – all rights reserved

per il badge di accesso ai locali. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette InfoCert.

5.4 Gestione del giornale di controllo

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

5.4.1 Tipi di eventi memorizzati

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

5.4.3 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per almeno 20 anni dalla CA. I log relativi al ciclo di vita del certificato rimangono in conservazione per almeno 20 anni dalla scadenza del certificato, fino ad un massimo di 23 anni dalla data di emissione.

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita dai servizi InfoCert di Conservazione a norma dei documenti informatici.

InfoCert S.p.A. – all rights reserved

5.4.5 Procedure di backup del giornale di controllo

I servizi InfoCert di Conservazione a norma dei documenti informatici 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 dai servizi InfoCert 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

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

5.5 Archiviazione dei verbali

5.5.1 Tipi di verbali archiviati

Vengono redatti e archiviati verbali relativi ai più importanti eventi di una Certification Authority. I verbali vengono conservati per 20 anni dalla Certification Authority a mezzo dei servizi InfoCert di Conservazione a norma dei documenti informatici.

5.5.2 Protezione dei verbali

La protezione è garantita dai servizi InfoCert di Conservazione a norma dei documenti informatici.

5.5.3 Procedure di backup dei verbali

I servizi InfoCert di Conservazione a norma dei documenti informatici attuano una politica e procedura di backup, come previsto dal manuale della sicurezza dei suddetti servizi.

InfoCert S.p.A. – all rights reserved

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 dai servizi InfoCert di Conservazione a norma dei documenti informatici e descritti nel manuale della sicurezza.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

I dati sono tutti conservati a mezzo dei servizi InfoCert di Conservazione a norma dei documenti informatici, i quali prevedono verifiche puntuali sullo stato del sistema e l'integrità dei dati. L'esibizione dei dati avviene secondo quanto stabilito dalla norma.

5.6 Sostituzione della chiave privata della CA

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

5.7 Compromissione della chiave privata della CA e disaster recovery

5.7.1 Procedure per la gestione degli incidenti

La CA ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27001. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirate a eliminare le cause che possono aver dato luogo all'incidente, se sotto il controllo di InfoCert conforme all'articolo 19 del Regolamento eIDAS.

InfoCert S.p.A. – all rights reserved

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 considerata un evento particolarmente critico, in quanto invaliderebbe i certificati emessi e le informazioni sullo stato di revoca 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.
Nonostante sia un evento raro, InfoCert ha predisposto una procedura dettagliata da seguire nell'ambito del SGSI certificato ISO 27001, dandone evidenza al CAB.
Una volta accertata la compromissione della chiave privata di CA, InfoCert procederà tempestivamente a:

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

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

5.8 Cessazione del servizio della CA o della RA

Nel caso di cessazione dell'attività di certificazione, InfoCert comunicherà questa intenzione all'Autorità di vigilanza (AgID) e l'ente di certificazione (CAB) con un anticipo di almeno 3 (tre) mesi, indicando, eventualmente, il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione. Con pari anticipo InfoCert informa della cessazione delle attività tutti i possessori di certificati

InfoCert S.p.A. – all rights reserved

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 conforme allo standard ETSI 319 411-1.
Maggiori dettagli sono presenti nel documento TSP Termination Plan dei Servizi di Certificazione Digitale, Validazione Temporale e Convalida firme disponibile presso il certificatore.

InfoCert S.p.A. – all rights reserved

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'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo tale che non sia possibile l'intercettazione del valore della chiave privata utilizzata.

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.
Nel caso in cui il dispositivo non sia messo a diposizione dalla CA, il Richiedente deve assicurare che il dispositivo rispetti la normativa vigente, presentando apposita documentazione ed essendo soggetto a audit periodici. Nel caso di HSM InfoCert si riserva di presiedere alla Key Ceremony.

InfoCert S.p.A. – all rights reserved

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. In alcuni casi, i dispositivi possono essere già nella disponibilità del Soggetto, consegnati preventivamente secondo procedure sicure e previa identificazione del Soggetto stesso.

6.1.3 Consegna della chiave pubblica alla CA

n/a

6.1.4 Consegna della chiave pubblica agli utenti

Se il Richiedente ne fa richiesta, escluso per i certificati LongTerm e OneShot, viene pubblicato anche nel registro pubblico, da dove può essere recuperato dall'Utente.

6.1.5 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche di certificazione è generata all'interno di un dispositivo crittografico hardware di cui sopra.
Le chiavi di root CA che firmano l'emissione di nuovi certificati possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 4096 bit;
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

Le chiavi del soggetto possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bits;
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

InfoCert S.p.A. – all rights reserved

6.1.6 Controlli di qualità e generazione della chiave pubblica

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

6.1.7 Scopo di utilizzo della chiave

6.1.7.1 Utilizzo chiave di CA

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

6.1.7.2 Utilizzo chiave del Titolare

Lo scopo di utilizzo della chiave del Titolare è determinato dall'estensione KeyUsage come definita nello standard X509. La maggior parte dei certificati descritti in questo Manuale Operativo contiene solamente il KeyUsage di "non ripudio". Sono ammesse delle eccezioni identificate con specifici OID per permettere anche la coppia "non ripudio" e "firma digitale" e la tripletta "non ripudio", "firma digitale" e "cifratura chiave". Quest'ultima tripletta è utilizzata ad esempio nell'ambito delle Pubbliche Amministrazioni Spagnole secondo i riferimenti normativi [17], [18], [19].

6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

6.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da InfoCert per le chiavi di certificazione (CA) e per il risponditore OCSP sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 in Europa.
Le smartcard utilizzate da InfoCert sono certificate come dispositivi qualificati (QSCD) secondo il regolamento eIDAS.
I moduli crittografici utilizzati da InfoCert per le chiavi di firma remota e automatica del Soggetto sono presenti nella lista dei QSCD notificati come definito dell'art. 3 del Regolamento eIDAS 910/2014.

InfoCert S.p.A. – all rights reserved

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 del 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, gestito dal Certificatore, che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende bloccato o rende illeggibile il dispositivo stesso.

6.2.8 Metodo di attivazione della chiave privata

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

InfoCert S.p.A. – all rights reserved

6.2.9 Metodo di disattivazione della chiave privata

n/a

6.2.10 Metodo per distruggere la chiave privata della CA

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

6.2.11 Classificazione dei moduli crittografici

n/a

6.3 Altri aspetti della gestione delle chiavi

n/a

6.3.1 Archiviazione della chiave pubblica

n/a

6.3.2 Periodo di validità del certificato e della coppia di chiavi

Il periodo di validità del certificato è determinato sulla base:

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

L'intervallo di validità del certificato è espresso al suo interno nella modalità indicata al paragrafo § 3.3.3.
Attualmente il certificato della CA ha una durata non superiore a 16 (sedici) anni, i certificati emessi a persona fisica o giuridica hanno validità non superiore ai 63 (sessantatre) mesi, compatibilmente con la robustezza degli algoritmi utilizzati.

6.4 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.3.3 e 6.3.

InfoCert S.p.A. – all rights reserved

6.5 Controlli sulla sicurezza informatica

6.5.1 Requisiti di sicurezza specifici dei computer

Il sistema operativo degli elaboratori utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, sono securizzati (hardening), sono cioè configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della CA.

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

6.6 Operatività sui sistemi di controllo

InfoCert attribuisce importanza strategica al trattamento sicuro delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità alla norma ISO/IEC 27001 per le attività EA:33-35.
Nel SGSI sono previsti procedure e controlli per:

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

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

6.7 Controlli di sicurezza della rete

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

InfoCert S.p.A. – all rights reserved

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

6.8 Sistema di validazione temporale

InfoCert fornisce un servizio di validazione temporale qualificato. Per la marcatura temporale occorre fare riferimento al Manuale Operativo ICERT-INDI-TSA presente sul sito di InfoCert.

InfoCert S.p.A. – all rights reserved

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 147/2019 [13]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.
InfoCert utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.
In 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 InfoCert 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

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

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

7.1.4 Forme di nomi

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

InfoCert S.p.A. – all rights reserved

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2.

7.2 Formato della CRL

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

7.2.1 Numero di versione

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

7.2.2 Estensioni della CRL

Per le estensioni della CRL si veda Appendice A.

7.3 Formato dell'OCSP

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

7.3.1 Numero di versione

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

7.3.2 Estensioni dell'OCSP

Per le estensioni dell'OCSP si veda Appendice A.

InfoCert S.p.A. – all rights reserved

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.
InfoCert 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.

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 InfoCert e CAB

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

8.4 Aspetti oggetto di valutazione

Il CAB è chiamato a valutare la conformità rispetto al Manuale Operativo, al

InfoCert S.p.A. – all rights reserved

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.
InfoCert si impegna a risolvere tutte le non conformità in maniera tempestiva, mettendo in atto tutte le azioni di miglioramento e adeguamento necessarie.

InfoCert S.p.A. – all rights reserved

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

9.1.1 Tariffe per il rilascio, il rinnovo e la riemissione con nuove chiavi dei certificati

In caso di certificati LongTerm o OneShot, di norma, i costi per l'emissione del certificato sono sostenuti dal Cliente diretto di InfoCert e non dal Soggetto, in base a tariffe definite dal contratto di servizi tra il Cliente e InfoCert.
Negli altri casi, le tariffe sono disponibili presso i siti https://www.firma.infocert.it/ e http://ecommerce.infocert.it, o presso le Registration Authority. La CA può stipulare accordi commerciali con le RA, e/o i Clienti prevedendo tariffe specifiche.

9.1.2 Tariffe per l'accesso ai certificati

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 i siti https://www.firma.infocert.it/ e http://ecommerce.infocert.it, o presso le Registration Authority.
La CA può stipulare accordi commerciali con le RA, e/o i Clienti prevedendo tariffe specifiche.

9.1.5 Politiche per il rimborso

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

InfoCert S.p.A. – all rights reserved

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

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

- 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 InfoCert in conformità a quanto indicato nel Codice

InfoCert S.p.A. – all rights reserved

dell'Amministrazione Digitale, nel Decreto Legislativo 30 giugno 2003, n. 196 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 [4].

9.4.1 Programma sulla privacy

InfoCert adotta un set di policy tramite le quali implementa e integra la protezione dei dati personali all'interno del suo Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001, condividendo con quest'ultimo sistema il processo di miglioramento continuo.

9.4.2 Dati che sono trattati come personali

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

9.4.3 Dati non considerati come personali

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

9.4.4 Titolare del trattamento dei dati personali

InfoCert S.p.A.
Piazza Sallustion n. 9
00147 Roma
richieste.privacy@legalmail.it

9.4.5 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy è disponibile sul sito www.infocert.it. InfoCert procede, se necessario, a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge [4] prima dell'erogazione del servizio. Informative specifiche possono essere presenti sul sito del Cliente, che, qualora necessario, potrebbe raccogliere il

InfoCert S.p.A. – all rights reserved

consenso al trattamento per conto di InfoCert.

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

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

9.4.7 Altri motivi di divulgazione

Non previsti.

9.5 Proprietà intellettuale

Il diritto d'autore sul presente documento è di InfoCert. Tutti i diritti sono riservati.

9.6 Rappresentanza e garanzie

InfoCert mantiene 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.
In quest'ultimo caso, la rappresentanza si esplica tramite mandato conferito da InfoCert 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 InfoCert.
Il Titolare è responsabile della veridicità dei dati comunicati nella Richiesta di Registrazione e Certificazione. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, sarà considerato responsabile di tutti i danni derivanti al Certificatore e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare il Certificatore da eventuali richieste di risarcimento danni.
Il Titolare 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).

InfoCert S.p.A. – all rights reserved

9.7 Limitazioni di garanzia

InfoCert 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).
InfoCert garantisce unicamente il funzionamento del Servizio, secondo i livelli indicati al paragrafo 9.15 del Manuale Operativo.

9.8 Limitazioni di responsabilità

InfoCert 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, InfoCert non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificati di sottoscrizione rilasciati in base alle previsioni del presente Manuale e delle Condizioni Generali dei Servizi di Certificazione.
InfoCert 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.
InfoCert, inoltre, fin dalla fase di formazione del Contratto per i servizi di Certificazione, e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e della rete internet.
InfoCert, 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 InfoCert.

InfoCert S.p.A. – all rights reserved

9.9 Indennizzi

InfoCert è unicamente responsabile degli eventuali danni direttamente determinati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica, in seguito a un mancato adempimento degli obblighi di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e dal mancato utilizzo, da parte di InfoCert, 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 InfoCert, 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, tra CA e RA, tra CA e Richiedente, il certificato viene revocato. La certificazione 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 sia mantenendo le stesse chiavi, sia ri-certificando nuove chiavi, secondo la procedura indicata dal presente Manuale Operativo. Il rinnovo comporta la proroga del contratto di certificazione fino alla scadenza o revoca del certificato rinnovato ed il pagamento dei corrispettivi stabiliti per tale servizio. Un certificato scaduto o revocato non può essere rinnovato.

9.10.2 Risoluzione

Il Contratto si risolverà di diritto con contestuale interruzione del Servizio e revoca

InfoCert S.p.A. – all rights reserved

del certificato emesso nelle ipotesi di mancato adempimento delle clausole tempo per tempo segnalate nel contratto di fornitura del servizio. La risoluzione si verificherà di diritto quando la parte interessata dichiari all'altra a mezzo PEC o lettera raccomandata a.r., che intende avvalersi della presente clausola.
In tutti i casi di risoluzione saranno salvi gli effetti prodotti dal Contratto fino a tale momento.
Il Titolare prende atto che, in caso di risoluzione del Contratto, per qualsiasi causa essa avvenga, non sarà più possibile usufruire del Servizio.

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata revoca del certificato.

9.10.4 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1.

9.10.5 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.

9.10.6 Storia delle revisioni

Versione/Release	**4.11**

InfoCert S.p.A. – all rights reserved

n°:	
Data Versione/Release:	15/05/2024
Descrizione modifiche:	§§ 1.2, 4.1.1: Precisazione con aggiunta sito istituzionale § 1.3.1: Revisione dati societari § 1.3.2.1: Precisazioni §§ 1.5.1, 4.9.3: Eliminazione fax dai contatti e revisione contatti § 1.5.2, 9.10.7: Aggiornamento denominazioni aree aziendali § 1.6.1 e 1.6.2: Aggiunta definizione di Cliente, armonizzazione definizioni e acronimi § 2.3.1, 2.3.2: precisazione sull'indirizzo di pubblicazione § 3.1.3: Revisione policy conservazione § 3.2.2: Precisazioni sull'uso di basi dati affidabili § 3.2.3: Precisazioni sulle modalità di riconoscimento § 4.5.3: Revisione limite d'uso § 4.9.3 e 4.9.5: Precisazioni sulla revoca § 5.1.1: Revisione descrizione § 5.1.3: Aggiornamento certificazione del sito § 5.1.7 e 5.1.8: Revisione descrizione § 6.2.1: Revisione descrizione § 6.6: Revisione descrizione § 8.3: Revisione descrizione § 9.2.1: Revisione descrizione § 9.4: Precisazioni § 9.4.4: Aggiornamento § 9.4.5: Revisione descrizione § 9.10.2: Revisione descrizione § 9.12: Revisione descrizione Revisione generale con correzioni ortografiche e grammaticali, riformulazioni e precisazioni
Motivazioni:	Revisione generale

Versione/Release n°:	**4.10**
Data	20/09/2023

InfoCert S.p.A. – all rights reserved

Versione/Release:	
Descrizione modifiche:	Chiarimenti SelfQ e Re-key
Motivazioni:	Richieste di riformulazione da parte di AgID

Versione/Release n°:	**4.9**
Data Versione/Release:	29/05/2023
Descrizione modifiche:	§§ 3.2.3, 3.2.3.5 Nuova modalità di riconoscimento
Motivazioni:	Nuova modalità di riconoscimento

Versione/Release n°:	**4.8**
Data Versione/Release:	18/04/2023
Descrizione modifiche:	Modifica logo InfoCert e formattazioni § 1.2 Aggiunta nuovi OID §§ 1.2, 3.1.1, 3.1.5, 3.2.4, 7.1, 9.15 Aggiunto riferimento a Determinazione AgID 147/2019 §§ 3.3, 4.6, 4.7, 9.1, 9.10 Precisazioni su rinnovo e ricertificazione chiavi § 3.2.3.1, 3.2.3.5 Aggiunta precisazioni §§ 5.1.1, 5.1.3, 5.1.5 Revisione aspetti di facility § 5.4.2 Revisione descrizione § 5.6 Correzione descrizione § 5.8 Modifica tempi di preavviso in caso di terminazione § 6.1.7.2 Modifica KeyUsage ammessi § Appendice A Aggiornamento formato CRL e OCSP
Motivazioni:	Revisione generale Rebranding

InfoCert S.p.A. – all rights reserved

Versione/Release n°:	**4.7**
Data Versione/Release:	17/03/2022
Descrizione modifiche:	§ 1.2 Revisione descrizioni nella tabella OID § 1.6.1 Revisione delle definizioni LongTerm e OneShot e introduzione dei certificati short-term § 3.1.1 Deroga a RFC 5280 per la lunghezza di alcuni campi del subjectDN § 3.1.5 Inserimento del codice LEI nei certificati a persona giuridica § 3.2.5 Correzione rimandi a paragrafi § 3.2.3 Aggiunta "Riconoscimento effettuato secondo la modalità 7 – ContoID" § 4.5.1 Revisione descrizione § 4.5.3 Revisione descrizione e aggiunta limite d'uso per certificati a persona giuridica con codice LEI per PoC § 4.9.3 Precisazioni per certificati short-term § 4.9.5 Rimodulazione tempistiche di evasione della richiesta di revoca § 4.9.9 Precisazione sulla coerenza di OCSP e CRL § 4.9.15 Precisazioni per certificati short-term § 5 Periodicità di revisione delle politiche di sicurezza § 5.4.3 Precisazione sul periodo di conservazione e §§ 5.4.4. 5.5 Aggiornamento descrizione § 6.1.2 Revisione descrizione § 6.4 Correzione rimando paragrafo § Appendice A Semplificazione descrizione delle estensioni del certificato Formattazione per accessibilità del documento
Motivazioni:	Revisione generale Modifica formattazione

Versione/Release n°:	**4.6**
Data Versione/Release:	10/09/2021

InfoCert S.p.A. – all rights reserved

Descrizione modifiche:	§ 1.5.1 Aggiornamento dei contatti
Motivazioni:	Modifica contatti

Versione/Release n°:	**4.5**
Data Versione/Release:	18/05/2021
Descrizione modifiche:	§ 3.1.1 Aggiunto dettaglio di applicazione della delibera Agid in base al contesto § 3.1.6 Aggiunte precisazioni sull'utilizzo di marchi registrati § 3.2.3, 3.2.3, 3.2.4, 3.2.5 Revisione organizzazione paragrafi § 3.2.3 Aggiunto riferimento a "CPS Addendum – Documenti di identità accettabili" § 3.2.3.3 Precisazioni su utilizzo della modalità SignID § 4.2.1, 4.2.2, 4.2.3 Revisione organizzazione paragrafi § 4.3.1 Aggiornamento descrizione § 4.5.3 Aggiunto riferimento ai limiti d'uso per i certificati Spagnoli § 4.9, 5.8 Chiarimento relativo alle informazioni sullo stato di revoca § 4.9.15.1 Aggiornamento descrizione § 5.1.1 Aggiornamento tecnologico § 5.3.5 Aggiornamento descrizione § 5.3.7 Aggiornamento descrizione § 5.8 Revisione descrizione § 5.5.6 Revisione descrizione § 6.1.5 e 7.1.3 Aggiornamento algoritmi e lunghezza delle chiavi § 6.1.7 Aggiornamento descrizione § 6.1.7.2 Aggiunta eccezione sullo scopo di utilizzo della chiave privata § 9.15 Aggiunte leggi di riferimento nel contesto Spagnolo e "CPS Addendum – Documenti di identità accettabili" § Appendice A Aggiunta nuova root CA § Appendice B Aggiornamento nome commerciale sw verifica

InfoCert S.p.A. – all rights reserved

	§ Appendice C Inserimento Certificato Qualificato del Cittadino Spagnolo Correzioni formali, aggiornamento definizioni, acronimi, riferimenti
Motivazioni:	Nuove root CA Revisione generale

Versione/Release n°:	**4.4**
Data Versione/Release:	10/02/2021
Descrizione modifiche:	§ 4.2.1 Aggiornamento relativo all'obbligatorietà e univocità di indirizzo e-mail e numero di cellulare § 4.2.2 Modalità di consegna elettronica della busta cifrata, come modalità predefinita § 4.9.13 Aggiunta la possibilità di una sospensione cautelativa a discrezione della CA
Motivazioni:	Richiesta AgID

Versione/Release n°:	**4.3**
Data Versione/Release:	15/06/2020
Descrizione modifiche:	§ 3.2.3 Aggiornamento elenco modalità di riconoscimento § 3.2.3.4 Riconoscimento identità da framework interoperabilità del nodo eIDAS § 3.2.3.5 Distinzione tra video assistito e non assistito con bonifico di rinforzo § 3.2.3.6 eDocID - Riconoscimento con documenti di identità elettronici § 4.5.3 Aggiornamento paragrafo con introduzione limiti d'uso per riconoscimenti di tipo autID e eDocID § 4.9.15 e § 4.9.16 chiarimenti sulla durata della sospensione
Motivazioni:	Allargamento modalità di riconoscimento Chiarimenti e typos

InfoCert S.p.A. – all rights reserved

Versione/Release n°:	4.2
Data Versione/Release:	24/03/2020
Descrizione modifiche:	§ 5.1.1 Aggiornamento tecnologico e riferimenti ai servizi ospitati su cloud AWS § 5.1.6 Aggiornamento tecnologico dei supporti di memorizzazione § Appendice A – inserimento della nuova root CA Electronic Signature Qualified Root "InfoCert Qualified Electronic Signature CA 4"
Motivazioni:	Nuova root CA

Versione/Release n°:	4.1
Data Versione/Release:	10/10/2019
Descrizione modifiche:	§ 3.1.5 Aggiunto la possibilità di usare come identificativo univoco quanto previsto dal documento eIDAS eID Profile di EiDAS cooperation network
Motivazioni:	-

Versione/Release n°:	4.0 (versione mai pubblicata, aggiornamenti riportati alla 4.1)
Data Versione/Release:	14/06/2019
Descrizione modifiche:	Correzioni formali, aggiornamento definizioni, acronimi, riferimenti § 1.2 Aggiornamento versione documento, descrizione OID agIDcert § 1.3.5 Aggiornamento per soggetto minorenne § 1.6.1 Introduzione definizioni Certificati OneShot, Certificati LongTerm e Dominio Informatico § 2.2.3 Aggiornamento CRL distribution points § 3.1.1 Aggiornamento per determinazione AgID 121/2019 § 3.1.5 Aggiornamento per determinazione AgID 121/2019

InfoCert S.p.A. – all rights reserved

	§ 3.2.6 Descrizione più chiara § 4.3.1.5 Descrizione certificati emessi con finalità di test §4.5.3 Aggiunto limite d'uso per emissione con SPID e aggiornata descrizione limite di valore § 4.9.2 Descrizione più chiara § 5.1.1 Chiarimento sulla sede del Data Center § 5.3.7 Compilata descrizione accessi fisici § 5.4.1 Aggiunti descrizione log accessi fisici e logici Accorpamento dei seguenti paragrafi dei due manuali: • § 2.2.2 Pubblicazione dei certificati • § 3.1.3 Anonimato e pseudonimia dei richiedenti • § 3.2.3.4 Riconoscimento effettuato secondo la modalità 4 – AUTID • § 4.1.1 Chi può richiedere un certificato • § 4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato • § 4.4.2Pubblicazione del certificato da parte della Certification Authority • § 4.5.1 Uso della chiave privata e del certificato da parte del Soggetto • § 4.6.1 Motivi per il rinnovo • § 4.9.3 Procedure per richiedere la revoca • § 4.9.15 Procedure per richiedere la sospensione • § 6.1.1 Generazione della coppia di chiavi del Soggetto • § 6.1.2 Consegna della chiave privata al Richiedente • § 6.1.4 Consegna della chiave pubblica agli Utenti • § 6.2.7 Memorizzazione della chiave privata su modulo crittografico • § 9.1.1 Tariffe per il rilascio ed il rinnovo dei certificati • § 9.4.5 Informativa privacy e consenso al trattamento dei dati personali • § 9.10.2 Risoluzione
Motivazioni:	Fusione del ICERT-INDI-MO, versione 3.5 del 30/11/2018 e ICERT-INDI-MO-ENT, versione 3.5 del 30/11/2018. Aggiornamento alla determinazione Agid 121/2019. Chiarimenti.

Versione/Release n°:	**3.5**
Data	30/11/2018

InfoCert S.p.A. – all rights reserved

Versione/Release:	
Descrizione modifiche:	§ 1.2 Aggiornamento OID e descrizione § 1.3 aggiornata ragione sociale del gruppo § 3.2.6 Identificazione persona giuridica PSP in ambito PSD2 § 4.2.1.2 Informazioni persona giuridica in ambito PSD2 § 4.9 Richiesta di revoca da parte dell'NCA per PSD2 Correzioni Typos e riferimenti
Motivazioni:	Emissione certificati di sigillo QSealC conformi direttiva PSD2 Cambio ragione sociale TecnoInvestimenti

Versione/Release n°:	**3.4**
Data Versione/Release:	20/06/2018
Descrizione modifiche:	§ 1.5.1 Modificato il numero del call center § 9.2.1 Aggiornati i massimali della copertura assicurativa
Motivazioni:	-

Versione/Release n°:	**3.3**
Data Versione/Release:	04/09/2918
Descrizione modifiche:	Cap. 1 Correzione di "firma digitale" in "firma elettronica qualificata". Alcune correzioni terminologiche per migliore comprensione, aggiunta di alcune definizioni di termini utilizzati nel documento § 3.1.5 Riscrittura parziale paragrafo per migliore comprensibilità § 3.2.3 Riscrittura tabella e sottoparagrafi per migliore chiarezza del contenuto e contestualizzazione su mercati europei. Estensione modalità 4 AutID a mezzi di identificazione elettronica di Stati Membri. Definizione di un documento specifico con tipologie di documenti e mezzi di identificazione elettronica accettati

InfoCert S.p.A. – all rights reserved

	§ 4.2 Riscrittura parziale paragrafo per migliore comprensibilità e contestualizzazione su mercati europei § 4.2.2 Ulteriori sistemi di autenticazione § 4.3.3.2 Possibilità di emissione di certificato già attivo § 4.5.3 Inserimento di un ulteriore limite d'uso § 4.9.15 e 4.9.16 Sospensione e riattivazione via CMS § 9.4 Aggiunta riferimenti a GDPR § 9.6, § 9.7, § 9.8, § 9.9, § 9.10 riscrittura paragrafi per migliore contestualizzazione Certificati utente: Aggiunti certificati persona giuridica su QSCD, corretti alcuni errori
Motivazioni:	-

Versione/Release n°:	**3.2**
Data Versione/Release:	02/05/2017
Descrizione modifiche:	Aggiunte informazioni relativa alla CA "Infocert Firma Qualificata 2" Aggiunti alcuni OID relativi alla CA "Infocert Firma Qualificata 2" Correzione forma e ortografia
Motivazioni:	

Versione/Release n°:	**3.1**
Data Versione/Release:	27/01/2017
Descrizione modifiche:	§3.2.3 eliminati tutti i riferimenti SPID come strumento di autenticazione per l'identificazione §3.2.3.1 dettagliato il riconoscimento da parte del datore di lavoro § 4.8.12 descritta la modalità di riattivazione della sospensione
Motivazioni:	-

InfoCert S.p.A. – all rights reserved

Versione/Release n°:	**3.0**
Data Versione/Release:	12/12/2016
Descrizione modifiche:	n/a
Motivazioni:	nuova emissione del documento

9.10.7 Procedure di revisione

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le revisioni sono apportate di concerto con il Responsabile del Servizio di Certificazione, il Responsabile della Sicurezza, il Responsabile della Privacy, il Responsabile Legale, il Responsabile Regulatory e approvate dalla Direzione Aziendale.

9.10.8 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

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

9.10.9 Casi nei quali l'OID deve cambiare

n/a

9.11 Risoluzione delle controversie

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

9.12 Foro competente

Si rimanda alla contrattualistica che regola il servizio per il dettaglio sul Foro competente.

InfoCert S.p.A. – all rights reserved

9.13 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] non utilizzato
[4] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018).
[5] non utilizzato.
[6] non utilizzato
[7] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori e relative normative nazionali di recepimento.
[8] Verifica preliminare - 24 settembre 2015 [4367555] Trattamento di dati personali nell'ambito del "Processo di rilascio con riconoscimento a mezzo webcam" per firma elettronica qualificata o digitale.
[9] Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determinazioni successive (dal 5 luglio 2019 sostituita da [13]).
[10] Determinazione AgID n. 189/2017.
[11] Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio, del 25 novembre 2015 conosciuta come Payment Services Directive – PSD2.
[12] Regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.
[13] Determinazione AgID n. 121/2019 ver 1.1 (sostituisce deliberazione CNIPA 45/2009) e successiva rettifica tramite Determinazione n. 147/2019.
[14] CPS Addendum – Documenti di identità accettabili.
[15] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
[16] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
[17] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

InfoCert S.p.A. – all rights reserved

[18] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
[19] Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza[10], nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].

9.14 Disposizioni varie

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

9.15 Altre disposizioni

Gli orari di erogazione del servizio, salvo accordi contrattuali diversi, sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (comprende i certificati CRL e OCSP).	Dalle 0:00 alle 24:00 7 giorni su 7 (disponibilità minima 99%)
Richiesta di Revoca e sospensione dei certificati.	Dalle 0:00 alle 24:00 7 giorni su 7 (disponibilità minima 99%)
Altre attività: registrazione, generazione, pubblicazione, rinnovo[11].	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi Dalle 9:00 alle 13:00 il sabato
Richiesta e/o verifica di marca temporale.	24hx7gg (disponibilità minima 99%)

[10] Disponibili sul sito https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata.
[11] L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono scegliere diversi orari di sportello. In ogni caso InfoCert garantisce l'erogazione del proprio servizio negli orari sopra riportati.

InfoCert S.p.A. – all rights reserved

APPENDICE A

Electronic Signature Qualified Root ”InfoCert Firma Qualificata 2”

```
 0 1318: SEQUENCE {
 4 1038:   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  133:     SEQUENCE {
34   11:       SET {
36    9:         SEQUENCE {
38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
43    2:           PrintableString 'IT'
      :         }
      :       }
47   21:       SET {
49   19:         SEQUENCE {
51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
56   12:           UTF8String 'INFOCERT SPA'
      :         }
      :       }
70   34:       SET {
72   32:         SEQUENCE {
74    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
79   25:           UTF8String 'Certificatore Accreditato'
      :         }
      :       }
106  20:       SET {
108  18:         SEQUENCE {
110   3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
115  11:           PrintableString '07945211006'
      :         }
      :       }
128  37:       SET {
130  35:         SEQUENCE {
132   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
137  28:           UTF8String 'InfoCert Firma Qualificata 2'
      :         }
      :       }
      :     }
167  30:     SEQUENCE {
169  13:       UTCTime 19/04/2013 14:26:15 GMT
184  13:       UTCTime 19/04/2029 15:26:15 GMT
      :     }
199 133:     SEQUENCE {
202  11:       SET {
204   9:         SEQUENCE {
206   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
211   2:           PrintableString 'IT'
      :         }
      :       }
215  21:       SET {
217  19:         SEQUENCE {
```

InfoCert S.p.A. – all rights reserved

```
219   3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
224  12:         UTF8String 'INFOCERT SPA'
     :        }
     :       }
238  34:     SET {
240  32:       SEQUENCE {
242   3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
247  25:         UTF8String 'Certificatore Accreditato'
     :        }
     :       }
274  20:     SET {
276  18:       SEQUENCE {
278   3:         OBJECT IDENTIFIER serialNumber (2 5 4 5)
283  11:         PrintableString '07945211006'
     :        }
     :       }
296  37:     SET {
298  35:       SEQUENCE {
300   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
305  28:         UTF8String 'InfoCert Firma Qualificata 2'
     :        }
     :       }
     :     }
335 290:   SEQUENCE {
339  13:     SEQUENCE {
341   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
352   0:       NULL
     :       }
354 271:     BIT STRING, encapsulates {
359 266:       SEQUENCE {
363 257:         INTEGER
     :           00 C5 A1 6E 5E 03 49 37 01 C5 3E FE FD AE 29 C9
     :           44 84 6A F1 5E 5A 8E 52 9B 40 40 92 D2 8F 2B 0F
     :           EC 86 8A 2A D1 B1 21 E5 FC 1C D6 AF C5 16 83 90
     :           B9 10 34 49 6A 97 EB 78 1A 02 0F C8 99 38 97 31
     :           DB 1F BD 9C D4 BB 36 48 7D 3A 5F BB 82 A3 98 86
     :           44 7D FE 15 4D 52 71 B7 2B CE F8 80 3C 1F B2 7A
     :           A5 19 D5 C2 A4 1B 2C 86 43 5C 01 B2 8A F1 A5 11
     :           14 79 A8 E4 5B 6C 2C 0E 26 3F 0D 8C 9E 4C 6D 48
     :               [ Another 129 bytes skipped ]
624   3:         INTEGER 65537
     :       }
     :     }
     :   }
629 413:   [3] {
633 409:     SEQUENCE {
637  15:       SEQUENCE {
639   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
644   1:         BOOLEAN TRUE
647   5:         OCTET STRING, encapsulates {
649   3:           SEQUENCE {
651   1:             BOOLEAN TRUE
     :           }
     :         }
     :       }
654  88:       SEQUENCE {
656   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
661  81:         OCTET STRING, encapsulates {
663  79:           SEQUENCE {
665  77:             SEQUENCE {
667   4:               OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
673  69:               SEQUENCE {
675  67:                 SEQUENCE {
```

InfoCert S.p.A. – all rights reserved

```
677   8:                 OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
687  55:                 IA5String
     :                   'http://www.firma.infocert.it/documentazione/manu'
     :                   'ali.php'
     :                   }
     :                  }
     :                 }
     :                }
     :               }
     :              }
744  37:         SEQUENCE {
746   3:          OBJECT IDENTIFIER issuerAltName (2 5 29 18)
751  30:          OCTET STRING, encapsulates {
753  28:           SEQUENCE {
755  26:            [1] 'firma.digitale@infocert.it'
     :             }
     :            }
     :           }
783 213:         SEQUENCE {
786   3:          OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
791 205:          OCTET STRING, encapsulates {
794 202:           SEQUENCE {
797 199:            SEQUENCE {
800 196:             [0] {
803 193:              [0] {
806  42:               [6]
     :                'http://crl.infocert.it/crls/firma2/ARL.crl'
850 146:               [6]
     :                'ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20'
     :                'Qualificata%202,ou%3DCertificatore%20Accreditato'
     :                ',o%3DINFOCERT%20SPA,c%3DIT?authorityRevocationLi'
     :                'st'
     :               }
     :              }
     :             }
     :            }
     :           }
     :          }
999  14:         SEQUENCE {
1001  3:          OBJECT IDENTIFIER keyUsage (2 5 29 15)
1006  1:          BOOLEAN TRUE
1009  4:          OCTET STRING, encapsulates {
1011  2:           BIT STRING 1 unused bit
     :            '1100000'B
     :           }
     :          }
1015 29:         SEQUENCE {
1017  3:          OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1022 22:          OCTET STRING, encapsulates {
1024 20:           OCTET STRING
     :            93 DD 21 FC 03 D0 15 0A 72 AD A3 CC D5 9A 09 9D
     :            38 8B 9D E9
     :           }
     :          }
     :         }
     :        }
     :       }
1046  13:  SEQUENCE {
1048   9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1059   0:   NULL
     :    }
1061 257:  BIT STRING
     :    96 1D 20 03 BC 24 21 EB F5 D4 D3 FE 4A 72 E4 06
```

InfoCert S.p.A. – all rights reserved

```
    :    69 82 8F 17 A0 84 16 FE AF 6D 35 03 F0 66 47 5D
    :    FD B0 1F 80 B8 9B A2 5B DB 93 B6 53 B2 25 65 56
    :    FD F9 05 BF 6B 84 CE 7C 48 A3 F5 5D AF 5C DB A0
    :    9F F3 2E 33 86 8A 65 55 B8 5F 29 11 95 08 B8 F5
    :    BB 51 17 74 F8 42 51 06 FC 59 67 0C D0 0C 8B 39
    :    78 F7 AA 16 CC 87 BE D4 2F 42 BD 79 A4 6B C1 30
    :    04 35 B9 78 DC 9C BA E4 73 C7 B9 B3 67 93 D5 3D
    :          [ Another 128 bytes skipped ]
     :  }
```

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature CA 3”

```
  0 1881: SEQUENCE {
  4 1345:   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  165:     SEQUENCE {
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'IT'
     :         }
     :       }
 47   24:       SET {
 49   22:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56   15:           UTF8String 'InfoCert S.p.A.'
     :         }
     :       }
 73   41:       SET {
 75   39:         SEQUENCE {
 77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   32:           UTF8String 'Qualified Trust Service Provider'
     :         }
     :       }
116   26:       SET {
118   24:         SEQUENCE {
120    3:           OBJECT IDENTIFIER '2 5 4 97'
125   17:           UTF8String 'VATIT-07945211006'
     :         }
     :       }
144   53:       SET {
146   51:         SEQUENCE {
148    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
153   44:           UTF8String
     :             'InfoCert Qualified Electronic Signature CA 3'
     :         }
     :       }
     :     }
199   30:     SEQUENCE {
201   13:       UTCTime 12/12/2016 16:34:43 GMT
```

InfoCert S.p.A. – all rights reserved

```
216  13:      UTCTime 12/12/2032 17:34:43 GMT
     :    }
231 165:   SEQUENCE {
234  11:    SET {
236   9:     SEQUENCE {
238   3:      OBJECT IDENTIFIER countryName (2 5 4 6)
243   2:      PrintableString 'IT'
     :      }
     :    }
247  24:    SET {
249  22:     SEQUENCE {
251   3:      OBJECT IDENTIFIER organizationName (2 5 4 10)
256  15:      UTF8String 'InfoCert S.p.A.'
     :      }
     :    }
273  41:    SET {
275  39:     SEQUENCE {
277   3:      OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282  32:      UTF8String 'Qualified Trust Service Provider'
     :      }
     :    }
316  26:    SET {
318  24:     SEQUENCE {
320   3:      OBJECT IDENTIFIER '2 5 4 97'
325  17:      UTF8String 'VATIT-07945211006'
     :      }
     :    }
344  53:    SET {
346  51:     SEQUENCE {
348   3:      OBJECT IDENTIFIER commonName (2 5 4 3)
353  44:      UTF8String
     :        'InfoCert Qualified Electronic Signature CA 3'
     :      }
     :    }
     :  }
399 546:  SEQUENCE {
403  13:    SEQUENCE {
405   9:     OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416   0:     NULL
     :    }
418 527:    BIT STRING, encapsulates {
423 522:     SEQUENCE {
427 513:      INTEGER
     :        00 B7 C1 D3 BF 11 CB A8 28 B6 91 DD E1 11 85 9F
     :        9D 9A 51 25 B3 B2 BC B2 AE AD DF 3E 5D 9F 5A A0
     :        F9 E4 64 C8 34 40 DA AB 7A EC 98 62 05 38 EC 91
     :        EA 84 F9 07 E6 58 DE 58 34 A0 EB 0D 11 19 50 BA
     :        E9 C0 13 C7 60 08 DB E5 AE 00 50 E9 7C 10 16 09
     :        9E 4D F4 EC 7B 14 99 6F D0 A4 67 68 CD 7D 88 1E
     :        D1 3E DA 25 BC 3C 66 61 8D B6 5D D6 F8 CF BA 7A
     :        55 96 86 62 CC 3F 9D D1 B0 2B 58 03 A7 21 49 BC
     :            [ Another 385 bytes skipped ]
944   3:      INTEGER 65537
     :      }
     :    }
     :  }
949 400:  [3] {
953 396:   SEQUENCE {
957  15:    SEQUENCE {
959   3:     OBJECT IDENTIFIER basicConstraints (2 5 29 19)
964   1:     BOOLEAN TRUE
967   5:     OCTET STRING, encapsulates {
969   3:      SEQUENCE {
```

InfoCert S.p.A. – all rights reserved

```
 971   1:           BOOLEAN TRUE
       :           }
       :          }
       :         }
 974  88:       SEQUENCE {
 976   3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 981  81:        OCTET STRING, encapsulates {
 983  79:         SEQUENCE {
 985  77:          SEQUENCE {
 987   4:           OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 993  69:           SEQUENCE {
 995  67:            SEQUENCE {
 997   8:             OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1007  55:               IA5String
       :              'http://www.firma.infocert.it/documentazione/manu'
       :              'ali.php'
       :               }
       :              }
       :             }
       :            }
       :           }
       :          }
1064 239:       SEQUENCE {
1067   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1072 231:        OCTET STRING, encapsulates {
1075 228:         SEQUENCE {
1078 225:          SEQUENCE {
1081 222:           [0] {
1084 219:            [0] {
1087  37:             [6] 'http://crl.infocert.it/ca3/qc/ARL.crl'
1126 177:              [6]
       :              'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
       :              'd%20Electronic%20Signature%20CA%203,ou%3DQualifi'
       :              'ed%20Trust%20Service%20Provider,o%3DINFOCERT%20S'
       :              'PA,c%3DIT?authorityRevocationList'
       :               }
       :              }
       :             }
       :            }
       :           }
       :          }
1306  14:       SEQUENCE {
1308   3:        OBJECT IDENTIFIER keyUsage (2 5 29 15)
1313   1:        BOOLEAN TRUE
1316   4:        OCTET STRING, encapsulates {
1318   2:         BIT STRING 1 unused bit
       :          '1100000'B
       :         }
       :        }
1322  29:       SEQUENCE {
1324   3:        OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1329  22:        OCTET STRING, encapsulates {
1331  20:         OCTET STRING
       :          9B 3B 1B 18 6A 3E A2 04 03 F4 D7 99 10 CF 97 11
       :          4C F1 AA DE
       :         }
       :        }
       :       }
       :      }
       :     }
1353  13:  SEQUENCE {
1355   9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1366   0:   NULL
```

InfoCert S.p.A. – all rights reserved

```
    :   }
1368  513:   BIT STRING
    :     54 49 DC F3 76 1F BF 5D 33 B7 78 3A 26 72 4B 2B
    :     50 79 22 70 4A 7E DA EB 8F 26 3C 7F 8D CB 08 8E
    :     96 A6 EB 00 93 5D 82 1D 48 C8 E0 FF C6 1D 69 32
    :     3F E8 F3 FC 7A C7 9C 33 4B 19 FA 13 37 01 7F 54
    :     12 49 A3 51 19 6C 3B 0C 50 F1 D2 97 83 7B CF 4F
    :     58 F4 82 27 98 FB C7 11 97 B8 D7 FC 73 F2 96 41
    :     D1 13 25 07 5A 77 B1 E4 BE 6C 0E BD FA D8 CA 58
    :     5B DC 4B 08 4F EC CC 9F CD E9 E8 9E 7D 43 27 4D
    :           [ Another 384 bytes skipped ]
    :   }
```

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature CA 4”

```
   0 1693: SEQUENCE {
   4 1157:   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  165:     SEQUENCE {
  34   11:       SET {
  36    9:         SEQUENCE {
  38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  43    2:           PrintableString 'IT'
     :         }
     :       }
  47   24:       SET {
  49   22:         SEQUENCE {
  51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
  56   15:           UTF8String 'InfoCert S.p.A.'
     :         }
     :       }
  73   41:       SET {
  75   39:         SEQUENCE {
  77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
  82   32:           UTF8String 'Qualified Trust Service Provider'
     :         }
     :       }
 116   26:       SET {
 118   24:         SEQUENCE {
 120    3:           OBJECT IDENTIFIER '2 5 4 97'
 125   17:           UTF8String 'VATIT-07945211006'
     :         }
     :       }
 144   53:       SET {
 146   51:         SEQUENCE {
 148    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 153   44:           UTF8String
     :             'InfoCert Qualified Electronic Signature CA 4'
     :         }
```

InfoCert S.p.A. – all rights reserved

```
    :       }
    :     }
199  30:   SEQUENCE {
201  13:     UTCTime 23/03/2020 09:21:16 GMT
216  13:     UTCTime 23/03/2036 10:21:16 GMT
    :     }
231 165:   SEQUENCE {
234  11:     SET {
236   9:       SEQUENCE {
238   3:         OBJECT IDENTIFIER countryName (2 5 4 6)
243   2:         PrintableString 'IT'
    :       }
    :     }
247  24:     SET {
249  22:       SEQUENCE {
251   3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
256  15:         UTF8String 'InfoCert S.p.A.'
    :       }
    :     }
273  41:     SET {
275  39:       SEQUENCE {
277   3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282  32:         UTF8String 'Qualified Trust Service Provider'
    :       }
    :     }
316  26:     SET {
318  24:       SEQUENCE {
320   3:         OBJECT IDENTIFIER '2 5 4 97'
325  17:         UTF8String 'VATIT-07945211006'
    :       }
    :     }
344  53:     SET {
346  51:       SEQUENCE {
348   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
353  44:         UTF8String
    :           'InfoCert Qualified Electronic Signature CA 4'
    :       }
    :     }
    :   }
399 546:   SEQUENCE {
403  13:     SEQUENCE {
405   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416   0:       NULL
    :     }
418 527:     BIT STRING, encapsulates {
423 522:       SEQUENCE {
427 513:         INTEGER
    :           00 B3 F6 00 3B 90 01 2E AC 2A 26 9E CB 03 0C 02
    :           E3 8A C3 14 FE F6 22 6B 6B B5 31 8E 44 8B 01 C2
    :           80 46 B8 E9 3B A6 84 84 4A AB 45 D4 60 D5 67 AF
    :           9D 57 BA DC EC AE AE AF 4F DD 71 4C 63 9E E2 81
    :           AF 71 16 A6 D2 4A C7 EE 7B EB 2B A4 18 14 6E 35
    :           C8 33 C6 BF AD 43 F9 10 90 97 73 A0 5C 87 B0 19
    :           5E 1E 87 E7 45 70 BE 68 19 EB 53 34 56 15 A5 D4
    :           84 57 6A AA 69 25 F0 48 1C 3A 59 B6 2B EF D9 68
    :           E3 CA 7D E6 39 30 BC BE 38 55 6A 08 D9 F7 B5 37
    :           8A ED B6 15 25 D3 E8 95 B3 3B 3F 7D B4 4F C0 EB
    :           D5 44 D4 A0 7E 93 4A 37 84 8D 2D 3B A2 77 44 48
    :           BC 29 F0 AE 98 85 0A 04 BE DD 3E 4A 73 BA 09 9A
    :           F9 9C DE B8 29 0D A2 E9 70 01 68 37 CB 53 36 80
    :           7B 04 C3 71 64 FE 20 91 B2 37 A1 B5 C7 B9 15 68
    :           C8 22 C5 C2 D8 DC 5D 7C F6 92 E7 D6 12 4B AA C6
    :           61 A9 C8 F3 FE E6 6C 89 8E A5 28 8A 20 7D D1 1F
```

InfoCert S.p.A. – all rights reserved

```
    :           A8 D4 34 A2 C0 24 E5 07 BB E3 1F AF 07 5C 46 AB
    :           1C 05 52 92 7B FE C4 C4 BD 87 66 FE 2F 4D F3 D9
    :           20 08 45 81 6E A0 03 A3 6E F7 38 DB A0 76 DD 8C
    :           D1 1F 0A E8 6E DB 6F 55 F0 EE 19 6D E7 AA 63 5C
    :           32 03 43 D1 F5 6C 08 16 93 DC 2D 00 B7 38 30 2F
    :           92 56 02 69 BA 0C 9E E2 B9 31 29 DB 2D 29 27 BF
    :           B1 94 9D 36 EE 2E 6F 2D E6 E8 43 17 93 E1 79 EB
    :           76 03 EB 30 7D 39 01 B0 6E 92 51 8D 1B 75 A3 7C
    :           E6 07 F2 24 96 DA 91 A6 5A AC 14 14 2D 8C 79 9C
    :           F4 CD 5A 78 A6 6A B2 7A 6D 2D 5C 78 91 D6 F6 D1
    :           0D 6E 24 4B A6 81 35 4C 58 E8 CA 21 B5 FA 7F 6C
    :           9A 03 45 51 DA F8 C8 17 2E 6B 95 3D F3 29 C7 DF
    :           80 AC 6D 59 B8 B9 6C 85 9F 9E EC CC 54 76 B4 94
    :           0A 0C 12 93 19 14 B2 E3 87 1D 9C 25 78 4C 9E 75
    :           70 B0 37 5F A9 EF EC 86 FD F8 5A 9B 5F A7 E6 85
    :           9E 5E DD 4A 98 58 86 8C 61 73 1D FF F0 C2 36 98
    :           99
 944   3:         INTEGER 65537
    :       }
    :      }
    :     }
 949 213:    [3] {
 952 210:      SEQUENCE {
 955  15:       SEQUENCE {
 957   3:        OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 962   1:        BOOLEAN TRUE
 965   5:        OCTET STRING, encapsulates {
 967   3:         SEQUENCE {
 969   1:          BOOLEAN TRUE
    :         }
    :        }
    :       }
 972  88:       SEQUENCE {
 974   3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 979  81:        OCTET STRING, encapsulates {
 981  79:         SEQUENCE {
 983  77:          SEQUENCE {
 985   4:           OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 991  69:           SEQUENCE {
 993  67:            SEQUENCE {
 995   8:             OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1005  55:               IA5String
    :             'http://www.firma.infocert.it/documentazione/manu'
    :             'ali.php'
    :            }
    :           }
    :          }
    :         }
    :        }
1062  54:       SEQUENCE {
1064   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1069  47:        OCTET STRING, encapsulates {
1071  45:         SEQUENCE {
1073  43:          SEQUENCE {
1075  41:           [0] {
1077  39:            [0] {
1079  37:             [6] 'http://crl.ca4.infocert.it/qc/ARL.crl'
    :            }
    :           }
    :          }
    :         }
    :        }
```

InfoCert S.p.A. – all rights reserved

```
    :         }
1118  14:       SEQUENCE {
1120   3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
1125   1:         BOOLEAN TRUE
1128   4:         OCTET STRING, encapsulates {
1130   2:           BIT STRING 1 unused bit
    :             '1100000'B
    :           }
    :         }
1134  29:       SEQUENCE {
1136   3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1141  22:         OCTET STRING, encapsulates {
1143  20:           OCTET STRING
    :             5D 7C 6B 61 E8 AC 90 EB 5E C9 D7 BE B4 E3 34 2E
    :             5C 2B 1C DF
    :           }
    :         }
    :       }
    :     }
    :   }
1165  13:   SEQUENCE {
1167   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1178   0:     NULL
    :     }
1180 513:   BIT STRING
    :     80 F2 2D 1C 50 0B 6C 38 DE 22 99 D7 69 5B 92 95
    :     99 AE FD FD 7A 3A 4D 06 D0 01 E3 CE 56 DC AF 5B
    :     A6 23 EB CD 35 DB 11 C0 72 27 79 E6 7B 91 E6 4F
    :     D5 77 D6 68 E3 D2 48 B3 E9 49 D6 5B D4 57 3F E0
    :     9E 46 E4 0E F4 CF 66 E6 28 6A 91 F1 BE 3F 42 44
    :     0E 75 EB A8 1A D4 24 2C 65 36 9B D5 1E 82 2B 45
    :     29 18 3A CC 91 51 66 69 7D FE 6E E2 63 94 DA E1
    :     E9 82 AE 9B CE 5E B9 7B 7C E3 08 97 94 DB 57 C9
    :     EC D1 9A 71 2B DE 25 2B 85 77 2B 7F 99 97 16 4D
    :     7B 84 A9 DF DA 75 C6 62 8B 3B 65 B3 C3 D7 5C 42
    :     BA AB FB CE 2D 6B AA B6 EB 6E AD EA 84 52 F1 0F
    :     C8 E0 64 9C A1 07 94 9E CF E0 22 E2 D1 3D 71 DD
    :     B5 90 6B D5 69 5E 86 7A BF 4D 6C 50 B5 EC CF 8F
    :     E4 15 DE 37 C8 5F CE 7A 8A 3E 52 C1 DE AB CF 08
    :     1B E9 8D 1D A0 14 8C A7 67 C0 77 3F A4 55 1C F3
    :     7A E9 CE 7D C1 99 BE D0 32 37 81 F9 39 95 AF 46
    :     EE B8 B3 22 16 9C AA 1D A2 EA F2 B1 67 93 3B 4B
    :     2F 71 80 91 5B CE 7F 0D EF F2 BD 31 73 C2 2A 8F
    :     E3 F1 B3 99 F0 97 10 4F DE 15 C9 B5 89 ED A7 14
    :     0B 57 96 70 AF 76 D2 F0 F9 5E 35 19 5E 4D 67 7F
    :     1E 23 D3 FA F6 6E CA DF B1 60 DE 35 38 81 08 21
    :     FF 7E 4E 06 3C 8E 75 55 78 AC 55 F0 73 40 84 D2
    :     76 97 FE 1E FE 42 E7 9D F3 69 5B BD 45 09 89 AF
    :     C9 11 A6 12 E0 E6 BB 34 87 51 21 78 38 FA 4B DA
    :     B9 57 6C 3A 85 65 01 DB 7D 27 64 89 C3 83 DD 44
    :     0B BF 91 46 EC 94 88 0A DB 7D 4F BD 79 5D 5E 2C
    :     07 D0 5D E0 87 6B 3E 68 4F 79 CA DF 1F 15 89 60
    :     C2 09 B9 4A 5F D6 D3 38 B0 F8 9A 4F 26 A4 34 D6
    :     62 9E 2A 7C 50 BF 43 7E AE F0 5C 31 F2 99 BE DD
    :     6B 97 12 E6 42 94 45 44 19 C0 01 33 E4 C8 FA 0B
    :     E2 BB D1 F2 A3 25 4A B8 58 12 C3 2A E9 BD 9C FF
    :     8D 31 41 5C 8D DC 55 9B B3 DB 9A 64 A0 56 14 8A
    :   }
```

InfoCert S.p.A. – all rights reserved

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature EC CA 4”

```
  0 872: SEQUENCE {
  4 751:   SEQUENCE {
  8   3:     [0] {
 10   1:       INTEGER 2
      :       }
 13  20:     INTEGER 0D 32 E7 F4 61 63 3C 34 DE 12 56 26 8E 51 91 97 08 F2 91 EF
 35  10:     SEQUENCE {
 37   8:       OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
      :       }
 47 168:     SEQUENCE {
 50  11:       SET {
 52   9:         SEQUENCE {
 54   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 59   2:           PrintableString 'IT'
      :         }
      :       }
 63  24:       SET {
 65  22:         SEQUENCE {
 67   3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 72  15:           UTF8String 'InfoCert S.p.A.'
      :         }
      :       }
 89  41:       SET {
 91  39:         SEQUENCE {
 93   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 98  32:           UTF8String 'Qualified Trust Service Provider'
      :         }
      :       }
132  26:       SET {
134  24:         SEQUENCE {
136   3:           OBJECT IDENTIFIER '2 5 4 97'
141  17:           UTF8String 'VATIT-07945211006'
      :         }
      :       }
160  56:       SET {
162  54:         SEQUENCE {
164   3:           OBJECT IDENTIFIER commonName (2 5 4 3)
169  47:           UTF8String
      :           'InfoCert Qualified Electronic Signature EC CA 4'
      :         }
      :       }
      :     }
218  30:     SEQUENCE {
220  13:       UTCTime 07/06/2021 08:43:18 GMT
235  13:       UTCTime 07/06/2036 09:43:18 GMT
      :     }
250 168:     SEQUENCE {
253  11:       SET {
255   9:         SEQUENCE {
257   3:           OBJECT IDENTIFIER countryName (2 5 4 6)
262   2:           PrintableString 'IT'
      :         }
      :       }
266  24:       SET {
268  22:         SEQUENCE {
```

InfoCert S.p.A. – all rights reserved

```
270  3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
275 15:         UTF8String 'InfoCert S.p.A.'
    :         }
    :       }
292 41:     SET {
294 39:       SEQUENCE {
296  3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
301 32:         UTF8String 'Qualified Trust Service Provider'
    :         }
    :       }
335 26:     SET {
337 24:       SEQUENCE {
339  3:         OBJECT IDENTIFIER '2 5 4 97'
344 17:         UTF8String 'VATIT-07945211006'
    :         }
    :       }
363 56:     SET {
365 54:       SEQUENCE {
367  3:         OBJECT IDENTIFIER commonName (2 5 4 3)
372 47:         UTF8String
    :           'InfoCert Qualified Electronic Signature EC CA 4'
    :         }
    :       }
    :     }
421 118:    SEQUENCE {
423  16:     SEQUENCE {
425   7:       OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
434   5:       OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
    :       }
441  98:     BIT STRING
    :       04 5A 3E C7 0A 5F EB BB 35 7B 85 FF B8 3C AD 7C
    :       D6 06 9B D0 A1 F9 6A E5 7F 95 9B D3 BE 74 E8 64
    :       D0 01 7F F2 B9 ED FF 8B 0C 97 66 6C 28 AC 26 20
    :       B1 28 96 F7 11 12 15 05 B9 94 75 FB CA 95 19 D0
    :       45 57 CD 7B 0E 7E DB A2 89 25 F1 F8 5A 4F 0B 59
    :       CF 9A 8C 68 9E C8 2E 69 56 94 5E 90 83 6F 9D 64
    :       FD
    :     }
541 215:    [3] {
544 212:      SEQUENCE {
547  15:       SEQUENCE {
549   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
554   1:         BOOLEAN TRUE
557   5:         OCTET STRING, encapsulates {
559   3:           SEQUENCE {
561   1:             BOOLEAN TRUE
    :           }
    :         }
    :       }
564  88:       SEQUENCE {
566   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
571  81:         OCTET STRING, encapsulates {
573  79:           SEQUENCE {
575  77:             SEQUENCE {
577   4:               OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
583  69:               SEQUENCE {
585  67:                 SEQUENCE {
587   8:                   OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
597  55:                   IA5String
    :                 'http://www.firma.infocert.it/documentazione/manu'
    :                 'ali.php'
    :                   }
    :                 }
```

InfoCert S.p.A. – all rights reserved

```
    :           }
    :          }
    :         }
    :        }
654  56:      SEQUENCE {
656   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
661  49:       OCTET STRING, encapsulates {
663  47:         SEQUENCE {
665  45:           SEQUENCE {
667  43:             [0] {
669  41:               [0] {
671  39:                 [6] 'http://crl.ca4.infocert.it/qcec/ARL.crl'
    :               }
    :             }
    :           }
    :          }
    :         }
    :        }
712  14:      SEQUENCE {
714   3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
719   1:       BOOLEAN TRUE
722   4:       OCTET STRING, encapsulates {
724   2:         BIT STRING 1 unused bit
    :           '1100000'B
    :         }
    :        }
728  29:      SEQUENCE {
730   3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
735  22:       OCTET STRING, encapsulates {
737  20:         OCTET STRING
    :           8C DF 7C B8 F0 94 15 36 0B 7F DF 81 71 F5 DB 41
    :           5D 3B FD FC
    :         }
    :        }
    :       }
    :      }
    :    }
759  10:  SEQUENCE {
761   8:    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
    :    }
771 103:  BIT STRING, encapsulates {
774 100:    SEQUENCE {
776  48:      INTEGER
    :       7C AF 22 1A 96 90 7C 55 72 88 49 DC B4 03 B6 7B
    :       E4 5F B2 2A CB 78 33 CC D6 EC 38 10 86 F4 21 41
    :       39 7B 78 EA 3D 59 10 BA BA 8C 30 E5 D6 09 2D FC
826  48:      INTEGER
    :       23 5D F8 C0 B2 26 9C D8 0D DA 64 EB 88 50 AB F2
    :       44 8F 85 BE 9A 59 7A C1 35 7A 66 4D 54 96 B1 60
    :       14 9A 2A C5 8D 63 93 A7 7B 14 78 8E AF 53 03 E3
    :      }
    :    }
    :  }
```

InfoCert S.p.A. – all rights reserved

Estensioni del certificato

Le estensioni contenute nei certificati emessi e la loro valorizzazione sono riportate nell'elenco che segue:

VERSION: contiene il valore 3 come descritto nel § 7.1.1
SERIALNUMBER: assegnato automaticamente dalla CA emittente
INNER SIGNATURE: § 7.1.3

ISSUER: contiene i seguenti campi valorizzati con il DN di una delle CA emittenti come riportato in § Appendice A:

CountryName
OrganizationName
OrganizationalUnitName
OrganizationIdentifier
CommonName

VALIDITY: massimo 63 (sessantatre) mesi, contiene i seguenti campi:

NotBefore
NotAfter

SUBJECT: contiene le informazioni relative al soggetto persona fisica o persona giuridica, può contenere i seguenti campi che sono soggetti a variazioni in relazione alla tipologia di certificato, ulteriori dettagli sono specificati al § 3.1:

Nel caso di certificato emesso a persona fisica:

CountryName: codice del Paese in base a ISO 3166.

OrganizationName: quando un soggetto persona fisica è associato a un'Organizzazione, il campo soggetto del certificato può identificare tale Organizzazione utilizzando gli attributi OrganizationName e OrganizationIdentifier

OrganizationalUnitName: se sono presenti gli attributi relativi all'Organizzazione, questo valore contiene ulteriori informazioni sull'Organizzazione stessa e può comparire non più di 4 (quattro) volte

OrganizationIdentifier: si veda definizione di OrganizationName, identificativo

InfoCert S.p.A. – all rights reserved

dell'Organizzazione a cui afferisce il soggetto, può essere valorizzato come definito al § 5.1.4 di ETSI EN 319 412-1 (es "VATIT-TaxIdentificationNumber", "NTRIT-IdentifierNationalTradeRegister)

GivenName: Nome del soggetto

Surname: Cognome del soggetto

SerialNumber: identificatore del soggetto; può essere valorizzato come definito al § 5.1.3 ETSI EN 319 412-1 e al § 3.1.5 del presente Manuale Operativo

Title: particolare qualifica o ruolo del soggetto, si veda § 3.2.4. del presente Manuale Operativo

LocalityName

DNQualifier: codice identificativo univoco all'interno della CA assegnato al soggetto

Pseudonym: valorizzato con lo pseudonimo del soggetto, se sono presenti GivenName e Surname questo valore non può essere presente.

CommonName: nome del soggetto persona fisica

Nel caso di certificato emesso a persona giuridica:

CountryName: codice del Paese in base a ISO 3166.

OrganizationName: denominazione registrata del soggetto persona giuridica

OrganizationIdentifier: identificativo dell'Organizzazione del soggetto, può essere valorizzato come definito al § 5.1.4 ETSI EN 319 412-1 e al § 3.1.5 del presente Manuale Operativo

CommonName: nome del soggetto persona giuridica

StateOrProvinceName

LocalityName

PUBLIC KEY: § 6.1.5

InfoCert S.p.A. – all rights reserved

EXTENSIONS:

AuthorityKeyIdentifier: permette di identificare la chiave pubblica corrispondente alla chiave privata utilizzata per firmare il certificato

KeyUsage: estensione marcata critica che definisce lo scopo della chiave contenuta nel certificato e segue le raccomandazioni ETSI EN 319 412–2 e ETSI EN 319 412–3

CRLDistributionPoints: contiene gli URL di pubblicazione delle CRL, si veda § 2.2.3

AuthorityInformationAccess: contiene le informazioni per accedere ai servizi della CA emittente, quali l'URL del servizio OCSP di validazione online (si veda § 7.3) e l'URL di pubblicazione del certificato di CA.

SubjectKeyIdentifier: contiene l'identificatore della chiave pubblica del certificato

SubjectDirectoryAttributes: può essere presente e contenere ulteriori attributi associate al soggetto:

DateOfBirth

SubjectAlternativeName: contiene indirizzi di posta elettronica, nomi DNS, indirizzi IP e URI legati al soggetto del certificato

RFC822Name: indirizzo e-mail del titolare

CertificatePolicies: contiene uno o più criteri costituiti da un OID e da qualificatori opzionali che indicano le policy in base alle quali il certificato è stato emesso e gli scopi per cui può essere utilizzato, si veda § 1.2, 4.5.3, contiene inoltre l'indirizzo di pubblicazione del presente Manuale Operativo (CPS).

qcStatements: (*Qualified Certificate Statements*) contengono un'estensione per l'inclusione di dichiarazioni che individuano peculiari proprietà del certificato:

QcCompliance (0.4.0.1862.1.1): contiene la dichiarazione di conformità alla normativa europea § 9.15 ed è presente in tutti i certificati emessi in conformità al presente Manuale Operativo.

QcEuLimitValue (0.4.0.1862.1.2): se previsto, contiene l'importo e la valuta come definito nel § 4.5.3

InfoCert S.p.A. – all rights reserved

QcEURetentionPeriod (0.4.0.1862.1.3): contiene il valore 20, inteso come numero di anni di conservazione delle evidenze come descritto nei § 3.1.3, 4.9, 5.4.3, 5.5.1

QcSSCD (0.4.0.1862.1.4): se presente, dichiara che la chiave privata relativa alla chiave pubblica contenuta nel certificato risiede in un Qualified Signature/Seal Creation Device (QSCD) vd. § 1.2

QcEuPDS (0.4.0.1862.1.5): contiene l'URL di pubblicazione della PKI Disclosure Statements (PDS)

QcType (0.4.0.1862.1.6): contiene uno tra i seguenti valori in base allo scopo per cui è emesso il certificato:
id-etsi-qct-esign
id-etsi-qct-eseal

pkixQCSyntax-v2 (1.3.6.1.5.5.7.0.18.11.2): se presente, contiene la semantica per attributi e nomi contenuti nei campi e nelle estensioni del certificato come definito da RFC3739:
id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1)
id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

SIGNATURE: § 7.1.3

InfoCert S.p.A. – all rights reserved

Estensioni QCStatement per QSealC PSD2

ETSI extensions: etsi-psd2-qcStatement (QcType)::= 0.4.0.19495.2	*SEQUENCE{* *rolesOfPSP RolesOfPSP,* *nCAName NCAName,* *nCAId NCAId }*
RolesOfPSP	*SEQUENCE{* *roleOfPspOid RoleOfPspOid,* *roleOfPspName RoleOfPspName }*
RoleOfPspOid	itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
RoleOfPspName	PSP_AS PSP_PI PSP_AI PSP_IC
NCAName	*plain text name in English of the NCA*
NCAId	• *2 character ISO 3166 country code representing the NCA country;* • *hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and* • *2-8 character NCA identifier without country code (A-Z uppercase only, no separator).*

Formato delle CRL e OCSP

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

InfoCert S.p.A. – all rights reserved

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

InfoCert S.p.A. – all rights reserved

Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Hash del DN dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente.
Serial Number	Numero di serie del certificato

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	Stato della rispsosta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificato firmatario della risposta OCSP.
Produced at	Data in formato GeneralizedTime di quando è stata generate la risposta OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Hash del distinguishName dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente
Serial Number	Numero di serie del certificato
thisUpdate	La data di verifica dello stato del certificato in formato GeneralizedTime
nextUpdate	Data in cui lo stato del certificato potrebbe essere aggiornato
Issuer Signature Algorithm	In base alla chiave del certificato di OCSP Responder, scelto tra sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-

InfoCert S.p.A. – all rights reserved

	SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer'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.

InfoCert S.p.A. – all rights reserved

Appendice B

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

InfoCert mette a disposizione un prodotto (denominato "GoSign") gratuitamente scaricabile dai Titolari dal sito www.firma.infocert.it per consentire:

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

Gli ambienti in cui GoSign opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo web sopra indicato. Le istruzioni per l'utilizzo del prodotto sono incluse nel prodotto stesso e consultabili tramite la funzione di help. Il prodotto GoSign è in grado di firmare qualsiasi tipo di file. La possibilità di visualizzare il file dipende dalla disponibilità sulla stazione di lavoro dell'utente di un adeguato software di visualizzazione.
InfoCert 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. documenti elettronici sottoscritti con certificati emessi da InfoCert possono essere verificati anche attraverso altri strumenti, in grado di interpretare i formati di firma previsti. Tali strumenti sono fuori dalla responsabilità di InfoCert.
Ad esempio, i documenti firmati utilizzando i certificati emessi in virtù del presente CPS, in formato PAdES, sono verificabili anche con lo strumento Adobe Reader®.

InfoCert S.p.A. – all rights reserved

Appendice C

Questa appendice contiene l'elenco e le caratteristiche dei certificati qualificati per la Spagna.
Al momento, l'unico certificato trattato è il certificato qualificato del Cittadino Spagnolo, che determina l'identità della persona fisica firmataria che agisce per proprio conto.
In termini generali, le Pubbliche Amministrazioni Spagnole richiedono che i certificati vengano rilasciati per i seguenti usi:

- Autenticazione basata su certificati X.509v3;
- Firma digitale, avanzata o qualificata, basata su certificati X.509v3;
- Crittografia asimmetrica o mista basata su certificati X.509v3.

I riferimenti normativi Spagnoli applicabili sono quelli compresi tra [15] e [19].

La policy per il certificato qualificato del Cittadino Spagnolo su dispositivo qualificato è la seguente:

Descrizione	OID
Manuale-operativo-certificato qualificato del "Cittadino Spagnolo" emesso a persona fisica e chiavi su dispositivo qualificato (QSCD)	**1.3.76.36.1.1.10.16.1.1.1** conforme alla policy QCP-n-qscd 0.4.0.194112.1.2

Certificato qualificato del Cittadino Spagnolo persona fisica su QSCD emesso dalla root CA "InfoCert Qualified Electronic Signature CA 4"

Field	Value
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 4
SUBJECT:	

InfoCert S.p.A. – all rights reserved

Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*)***
GivenName:	*Name (mandatory)*
Surname:	*Surname**s** (mandatory)*
SerialNumber:	*as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINES**-NIF or NIE", "**PASES-**PassportNumber", "**IDCES-**DNI or TIE CardNumber") (mandatory)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Common Name	*<DNI or NIE of the subject> + "" + <Name of the subject> <First Surname of the subject> (mandatory)*
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Directory Name	*(mandatory)*
	*Certificate holder **name** (mandatory) (OID 1.3.6.1.4.1.17326.30.7)*
	*Certificate holder **First Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.8)*
	*Certificate holder **Second Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.9)*
	*Certificate **Description** (mandatory) (OID 1.3.6.1.4.1.17326.30.10) ("CERTIFICADO ELECTRONICO CUALIFICADO DE CIUDADANO")*
User Notice	*Certificado cualificado de Ciudadano. Consulte las condiciones de uso en http://www.firma.infocert.it/documentazione/manuali.php (mandatory)*

(*): it contains the country consistent with the legal Jurisidction under which the certificate is issued

InfoCert S.p.A. – all rights reserved

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.

InfoCert S.p.A. – all rights reserved