Manuale Operativo Enterprise

Certificate Policy - Certificate Practice Statement

CODICE DOCUMENTO	ICERT-INDI-MO-ENT
VERSIONE	3.2
DATA	02/05/2017

InfoCert
GRUPPO TECNOINVESTIMENTI

SOMMARIO

1 INTRODUZIONE 7
1.1 Quadro generale 7
1.2 Nome ed identificativo del documento 7
1.3 Partecipanti e responsabilità 8
1.3.1 Certification Authority – Autorità di Certificazione 8
1.3.2 Registration authority – Ufficio di Registrazione (RA) 9
1.3.3 Soggetto 10
1.3.4 Utente 10
1.3.5 Richiedente 10
1.3.6 Autorità 10
1.4 Uso del certificato 11
1.4.1 Usi consentiti 11
1.4.2 Usi non consentiti 11
1.5 Amministrazione del Manuale Operativo 11
1.5.1 Contatti 11
1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo 11
1.5.3 Procedure di approvazione 12
1.6 Definizioni e acronimi 12
1.6.1 Definizioni 12
1.6.2 Acronimi e abbreviazioni 15
2 PUBBLICAZIONE E ARCHIVIAZIONE 18
2.1 Archiviazione 18
2.2 Pubblicazione delle informazioni sulla certificazione 18
2.2.1 Pubblicazione del manuale operativo 18
2.2.2 Pubblicazione dei certificati 18
2.2.3 Pubblicazione delle liste di revoca e sospensione 18
2.3 Periodo o frequenza di pubblicazione 18
2.3.1 Frequenza di pubblicazione del manuale operativo 18
2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione 19
2.4 Controllo degli accessi agli archivi pubblici 19
3 IDENTIFICAZIONE E AUTENTICAZIONE 20
3.1 Denominazione 20
3.1.1 Tipi di nomi 20
3.1.2 Necessità che il nome abbia un significato 20
3.1.3 Anonimato e pseudonimia dei richiedenti 20
3.1.4 Regole di interpretazione dei tipi di nomi 20
3.1.5 Univocità dei nomi 20
3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati 20
3.2 Convalida iniziale dell'identità 21
3.2.1 Metodo per dimostrare il possesso della chiave privata 21
3.2.2 Autenticazione dell'identità delle organizzazioni 21
3.2.3 Identificazione della persona fisica 21
3.2.4 Identificazione della persona giuridica 25
3.2.5 Informazioni del Soggetto o del Richiedente non verificate 25
3.2.6 Validazione dell'autorità 25
3.3 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati 25
3.3.1 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati 25
3.4 Identificazione e autenticazione per le richieste di revoca o sospensione 25
3.4.1 Richiesta da parte del Soggetto 25

3.4.2 Richiesta da parte del Richiedente ... 26
4 OPERATIVITÀ ... 27
4.1 Richiesta del certificato ... 27
4.1.1 Chi può richiedere un certificato ... 27
4.1.2 Processo di registrazione e responsabilità ... 27
4.2 Elaborazione della richiesta ... 28
4.2.1 Informazioni che il Soggetto deve fornire ... 28
4.2.2 Esecuzione delle funzioni di identificazione e autenticazione ... 28
4.2.3 Approvazione o rifiuto della richiesta del certificato ... 28
4.2.4 Tempo massimo per l'elaborazione della richiesta del certificato ... 29
4.3 Emissione del certificato ... 29
4.3.1 Azioni della CA durante l'emissione del certificato ... 29
4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato ... 29
4.3.3 Attivazione ... 29
4.4 Accettazione del certificato ... 29
4.4.1 Comportamenti concludenti di accettazione del certificato ... 29
4.4.2 Pubblicazione del certificato da parte della Certification Authority ... 29
4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato ... 30
4.5 Uso della coppia di chiavi e del certificato ... 30
4.5.1 Uso della chiave privata e del certificato da parte del Soggetto ... 30
4.5.2 Uso della chiave pubblica e del certificato da parte degli Utenti Finali ... 30
4.5.3 Limiti d'uso e di valore ... 30
4.6 Rinnovo del certificato ... 31
4.6.1 Motivi per il rinnovo ... 31
4.6.2 Chi può richiedere il rinnovo ... 31
4.6.3 Elaborazione della richiesta di rinnovo del certificato ... 31
4.7 Riemissione del certificato ... 32
4.8 Modifica del certificato ... 32
4.9 Revoca e sospensione del certificato ... 32
4.9.1 Motivi per la revoca ... 32
4.9.2 Chi può richiedere la revoca ... 32
4.9.3 Procedure per richiedere la revoca ... 32
4.9.4 Periodo di grazia della richiesta di revoca ... 33
4.9.5 Tempo massimo di elaborazione della richiesta di revoca ... 33
4.9.6 Frequenza di pubblicazione della CRL ... 34
4.9.7 Latenza massima della CRL ... 34
4.9.8 Servizi online di verifica dello stato di revoca del certificato ... 34
4.9.9 Motivi per la sospensione ... 34
4.9.10 Chi può richiedere la sospensione ... 34
4.9.11 Procedure per richiedere la sospensione ... 34
4.9.12 Limiti al periodo di sospensione ... 35
4.10 Servizi riguardanti lo stato del certificato ... 36
4.10.1 Caratteristiche operative ... 36
4.10.2 Disponibilità del servizio ... 37
4.10.3 Caratteristiche opzionali ... 37
4.11 Disdetta dai servizi della CA ... 37
4.12 Deposito presso terzi e recovery della chiave ... 37
5 MISURE DI SICUREZZA E CONTROLLI ... 38
5.1 Sicurezza fisica ... 38
5.1.1 Posizione e costruzione della struttura ... 38
5.1.2 Accesso fisico ... 39
5.1.3 Impianto elettrico e di climatizzazione ... 39
5.1.4 Prevenzione e protezione contro gli allagamenti ... 40
5.1.5 Prevenzione e protezione contro gli incendi ... 40
5.1.6 Supporti di memorizzazione ... 40
5.1.7 Smaltimento dei rifiuti ... 41

5.1.8 Off-site backup 41
5.2 Controlli procedurali 41
5.2.1 Ruoli chiave 41
5.3 Controllo del personale 41
5.3.1 Qualifiche, esperienze e autorizzazioni richieste 41
5.3.2 Procedure di controllo delle esperienze pregresse 41
5.3.3 Requisiti di formazione 41
5.3.4 Frequenza di aggiornamento della formazione 42
5.3.5 Frequenza nella rotazione dei turni di lavoro 42
5.3.6 Sanzioni per azioni non autorizzate 42
5.3.7 Controlli sul personale non dipendente 42
5.3.8 Documentazione che il personale deve fornire 42
5.4 Gestione del giornale di controllo 43
5.4.1 Tipi di eventi memorizzati 43
5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo 43
5.4.3 Periodo di conservazione del giornale di controllo 43
5.4.4 Protezione del giornale di controllo 43
5.4.5 Procedure di backup del giornale di controllo 43
5.4.6 Sistema di memorizzazione del giornale di controllo 43
5.4.7 Notifica in caso di identificazione di vulnerabilità 44
5.4.8 Valutazioni di vulnerabilità 44
5.5 Archiviazione dei verbali 44
5.5.1 Tipi di verbali archiviati 44
5.5.2 Protezione dei verbali 44
5.5.3 Procedure di backup dei verbali 44
5.5.4 Requisiti per la marcatura temporale dei verbali 44
5.5.5 Sistema di memorizzazione degli archivi 44
5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi 44
5.6 Sostituzione della chiave privata della CA 45
5.7 Compromissione della chiave privata della CA e disaster recovery 45
5.7.1 Procedure per la gestione degli incidenti 45
5.7.2 Corruzione delle macchine, del software o dei dati 45
5.7.3 Procedure in caso di compromissione della chiave privata della CA 45
5.7.4 Erogazione dei servizi di CA in caso di disastri 45
5.8 Cessazione del servizio della CA o della RA 45
6 CONTROLLI DI SICUREZZA TECNOLOGICA 47
6.1 Installazione e generazione della coppia di chiavi di certificazione 47
6.1.1 Generazione della coppia di chiavi del Soggetto 47
6.1.2 Consegna della chiave privata al Richiedente 47
6.1.3 Consegna della chiave pubblica alla CA 48
6.1.4 Consegna della chiave pubblica agli utenti 48
6.1.5 Algoritmo e lunghezza delle chiavi 48
6.1.6 Controlli di qualità e generazione della chiave pubblica 48
6.1.7 Scopo di utilizzo della chiave 48
6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico 49
6.2.1 Controlli e standard del modulo crittografico 49
6.2.2 Controllo di più persone della chiave privata di CA 49
6.2.3 Deposito presso terzi della chiave privata di CA 49
6.2.4 Backup della chiave privata di CA 49
6.2.5 Archiviazione della chiave privata di CA 49
6.2.6 Trasferimento della chiave privata da un modulo o su un modulo crittografico 49
6.2.7 Memorizzazione della chiave privata su modulo crittografico 49
6.2.8 Metodo di attivazione della chiave privata 50
6.2.9 Metodo di disattivazione della chiave privata 50
6.2.10 Metodo per distruggere la chiave privata della CA 50
6.2.11 Classificazione dei moduli crittografici 50

6.3 Altri aspetti della gestione delle chiavi....50
6.3.1 Archiviazione della chiave pubblica....50
6.3.2 Periodo di validità del certificato e della coppia di chiavi....50
6.4 Dati di attivazione della chiave privata....50
6.5 Controlli sulla sicurezza informatica....51
6.5.1 Requisiti di sicurezza specifici dei computer....51
6.6 Operatività sui sistemi di controllo....51
6.7 Controlli di sicurezza della rete....51
6.8 Controlli di sicurezza della rete....52
7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP....53
7.1 Formato del certificato....53
7.1.1 Numero di versione....53
7.1.2 Estensioni del certificato....53
7.1.3 OID dell'algoritmo di firma....53
7.1.4 Forme di nomi....53
7.1.5 Vincoli ai nomi....53
7.1.6 OID del certificato....53
7.2 Formato della CRL....53
7.2.1 Numero di versione....54
7.2.2 Estensioni della CRL....54
7.3 Formato dell'OCSP....54
7.3.1 Numero di versione....54
7.3.2 Estensioni dell'OCSP....54
8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ....55
8.1 Frequenza o circostanze per la valutazione di conformità....55
8.2 Identità e qualifiche di chi effettua il controllo....55
8.3 Rapporti tra InfoCert e CAB....55
8.4 Aspetti oggetto di valutazione....56
8.5 Azioni in caso di non conformità....56
9 ALTRI ASPETTI LEGALI E DI BUSINESS....57
9.1 Tariffe....57
9.1.1 Tariffe per il rilascio dei certificati....57
9.1.2 Tariffe per l'accesso ai certificati....57
9.1.3 Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati....57
9.1.4 Tariffe per altri servizi....57
9.1.5 Politiche per il rimborso....57
9.2 Responsabilità finanziaria....57
9.2.1 Copertura assicurativa....57
9.2.2 Altre attività....58
9.2.3 Garanzia o copertura assicurativa per i soggetti finali....58
9.3 Confidenzialità delle informazioni di business....58
9.3.1 Ambito di applicazione delle informazioni confidenziali....58
9.3.2 Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali....58
9.3.3 Responsabilità di protezione delle informazioni confidenziali....58
9.4 Privacy....58
9.4.1 Programma sulla privacy....58
9.4.2 Dati che sono trattati come personali....58
9.4.3 Dati non considerati come personali....59
9.4.4 Responsabilità di protezione dei dati personali....59
9.4.5 Informativa privacy e consenso al trattamento dei dati personali....59
9.4.6 Divulgazione dei dati a seguito di richiesta da parte dell'autorità....59
9.4.7 Altri motivi di divulgazione....59
9.5 Proprietà intellettuale....59
9.6 Rappresentanza e garanzie....59
9.7 Limitazione di garanzia....60
9.8 Limitazione di responsabilità....60

9.9 Indennizzi……60
9.10 Termine e risoluzione……..60
9.10.1 Termine..... 60
9.10.2 Risoluzione 60
9.10.3 Effetti della risoluzione..... 60
9.11 Canali di comunicazione ufficiali……60
9.12 Revisione del Manuale Operativo……..60
9.12.1 Storia delle revisioni..... 61
9.12.2 Procedure di revisione 61
9.12.3 Periodo e meccanismo di notifica..... 62
9.12.4 Casi nei quali l'OID deve cambiare 62
9.13 Risoluzione delle controversie……62
9.14 Foro competente……..62
9.15 Legge applicabile……..62
9.16 Disposizioni varie……..63
9.17 Altre disposizioni……...63
Certificato qualificato persona fisica con identificatori e chiavi semantiche su QSCD……...67
Certificato qualificato persona fisica SENZA identificatori e chiavi semantiche su QSCD emesso dalla CA "InfoCert Qualified Electronic Signature CA 3"……...70
Certificato qualificato persona fisica SENZA identificatori e chiavi semantiche su QSCD emesso dalla CA "InfoCert Qualified Electronic Signature CA 3"……...73
Avvertenza……78

INDICE DELLE FIGURE

Figura 1 - ubicazione Data Center InfoCert e sito della Disaster Recovery..... 39

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, e si applica ai processi di emissione di certificati qualificati per procedure di firma remota **Enterprise**: questi certificati qualificati sono utilizzati nell'ambito di processi di sottoscrizione di documenti informatici in vari contesti di mercato, al fine di semplificare i processi di business, e sono tecnicamente utilizzabili solamente nel contesto del **dominio informatico** nel quale sono stati emessi. Per brevità, nel proseguo del documento ci si riferirà a questi certificati con il termine **LongTerm.**
Il documento regolamenta anche le modalità di emissione dei certificati **OneShot**: si tratta di certificati validi per un breve periodo, la cui coppia di chiavi ha un utilizzo limitato esclusivamente alla transazione di firma per la quale sono stati emessi e nell'ambito di un determinato dominio informatico.

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

1.2 Nome ed identificativo del documento

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

sono identificabili in calce ad ogni pagina.

La versione 3.0 del presente documento si pone in continuità e sostituisce i previgenti Manuali Operativi denominati:

- ICERT-INDI-MO-REMOTE, versione 1.3 del 03/11/2016, per le parti che regolano l'emissione di certificati qualificati di firma remota LongTerm utilizzabili nell'ambito di un dominio informatico;
- ICERT-INDI-MO-SHOT, versione 2.2 del 03/11/2016, per le parti che regolano l'emissione di certificati qualificati di firma remota 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

Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo qualificato	1.3.76.36.1.1.35/1.3.76.36.1.1.65 conforme alla policy QCP-n-qscd 0.4.0.194112.2
Manuale-operativo-certificato qualificato emesso a persona fisica per firma remota su dispositivo qualificato di tipo one-shot	1.3.76.36.1.1.34/1.3.76.36.1.1.64 conforme alla policy QCP-n-qscd 0.4.0.194112.2

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo 4.5.3. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del Manuale Operativo.
Questo documento è pubblicato in formato elettronico presso il sito Web del Prestatore di Servizi Fiduciari all'indirizzo: http://www.firma.infocert.it, sezione "Documentazione".

1.3 Partecipanti e responsabilità

1.3.1 Certification Authority – Autorità di Certificazione

La **Certification Authority** è il soggetto terzo e fidato che emette i certificati qualificati di firma digitale, firmandoli con la propria chiave privata, detta chiave di CA o chiave di root.
InfoCert è la Certification Authority (**CA**) che emette, pubblica nel registro e revoca i Certificati 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 Tecnoinvestimenti S.p.A.
Sede legale	Piazza Sallustio n.9, 00187, Roma (RM)
Sede operativa	Via Marco e Marcelliano n.45, 00147, Roma (RM)
Rappresentante legale	Danilo Cattaneo In qualità di Amministratore Delegato
N. di telefono	06 836691
N. Iscrizione Registro Imprese	Codice Fiscale 07945211006
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** 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 di generazione dei codici OTP, ove previsto dal processo e come regolato dal contratto,
- l'attivazione della procedura di certificazione della chiave pubblica,
- la fornitura di supporto al Soggetto, al Richiedente e alla CA nelle eventuali fasi di 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, detto "Convenzione RAO", regolamenta il tipo di attività affidate dalla CA alla RA e le modalità operative di svolgimento.
Le RA sono attivate dalla CA a seguito di un adeguato addestramento del personale impiegato; la CA verifica la rispondenza delle procedure utilizzate a quanto stabilito dal presente Manuale.

1.3.2.1 Incaricato alla Registrazione (IR)

La RA può nominare, utilizzando la modulistica messa a disposizione dalla CA, persone fisiche o giuridiche cui affidare lo svolgimento delle attività di identificazione del Soggetto. Gli **Incaricati alla**

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

1.3.3 Soggetto

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

1.3.5 Richiedente

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

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

Se non specificato altrimenti nella documentazione contrattuale, il Richiedente coincide con il Soggetto.

1.3.6 Autorità

1.3.6.1 Agenzia per l'Italia Digitale - AgID

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

1.3.6.2 Organismo di valutazione della conformità - Conformity Assessment Body

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

1.4 Uso del certificato

1.4.1 Usi consentiti

I certificati emessi dalla CA InfoCert, secondo le modalità indicate dal presente manuale operativo, sono Certificati Qualificati ai sensi del CAD e dell'articolo 28 del Regolamento eIDAS.

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

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

1.4.2 Usi non consentiti

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel Manuale Operativo e 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 all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telefono: 06 836691
Fax: 049 0978914
Call Center Firma Digitale: 199.500.130
Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

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

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle Policies, dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dall'Ufficio Legale e

dall'Area di Consulenza e approvato dal management aziendale.

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2008.
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.
CAB – Conformity Assessment Body (Organismo di valutazione della conformità)	Organismo accreditato a norma del Regolamento eIDAS come competente ad effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
CAR – Conformity Assessment Report (Relazione di valutazione della conformità)	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr eIDAS [1]).
Certificato di firma elettronica	Un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona (cfr eIDAS [1]).
Certificato qualificato di firma elettronica	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (cfr eIDAS [1]).
Certificato LongTerm	Il certificato qualificato di firma digitale per procedura remota disciplinato nel presente Manuale Operativo, utilizzabile per firmare nell'ambito di un dominio informatico, in tutto il suo periodo di validità.
Certificato OneShot	Si intende certificato qualificato di firma digitale per procedura remota disciplinato nel presente Manuale Operativo le cui chiavi, una volta generate, sono disponibili solo nell'ambito di un dominio informatico ed esclusivamente per la transazione di firma per la quale è stato emesso. Immediatamente dopo al suo utilizzo la chiave privata viene distrutta.

Termine	Definizione
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 digitale 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 digitale apposta sul documento informatico dal Soggetto (cfr CAD [2]).
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 (cfr eIDAS [1]).
Dati di convalida	Dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1]).
Dati di identificazione personale	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr eIDAS [1]).
Dati per la creazione di una firma elettronica	I dati unici utilizzati dal firmatario per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica	Un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica qualificata (SSCD – secure system creation device o QSCD)	Un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS (cfr eIDAS [1]). L'iniziale Q sta a intendere che il dispositivo è qualificato.
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1]).
Dominio informatico	Si identifica con le pagine web relative alle applicazioni per il 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 pagine web 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.
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]).

Termine	Definizione
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr eIDAS [1]).
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse (cfr DPCM [5]).
Firmatario	Una persona fisica che crea una firma elettronica (cfr eIDAS [1]).
Giornale di controllo	Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [5].
Identificazione elettronica	Il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica (cfr eIDAS [1]).
Lista dei certificati revocati o sospesi [Certificate Revocation List - CRL]	È una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel registro pubblico.
Manuale operativo [certificate practice statement]	Il Manuale operativo definisce le procedure che la CA applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr eIDAS [1]).
Online Certificate Status Protocol (OCSP)	Protocollo definito dallo IETF nella RFC 6960, consente alle applicazioni di verificare la validità del certificato in maniera più veloce e puntuale rispetto alla CRL, di cui condivide i dati.
OTP - One Time Password:	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Soggetto in un momento immediatamente antecedente all'apposizione della firma digitale. Può essere basato su dispositivi hardware o su procedure software.
Parte facente affidamento sulla certificazione	Una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario (cfr eIDAS [1]).
Prestatore di servizi fiduciari	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato (cfr eIDAS [1]).
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.

Termine	Definizione
Registro pubblico [Directory]	Il Registro pubblico è un archivio che contiene: ▪ tutti i certificati emessi dalla CA per i quali sia stata richiesta dal Soggetto la pubblicazione; ▪ la lista dei certificati revocati e sospesi (CRL).
Revoca o sospensione di un certificato	È l'operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
Servizio fiduciario	Un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1]).
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1]).
Tempo Universale Coordinato [Coordinated Universal Time]	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento (cfr eIDAS [1]).
Validazione temporale elettronica qualificata	Una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS (cfr eIDAS [1]).
WebCam	Videocamera di ridotte dimensioni, destinata a trasmettere immagini in streaming via Internet e catturare immagini fotografiche. Collegata a un PC o integrata in dispositivi mobile è utilizzata per chat video o per videoconferenze.

1.6.2 Acronimi e abbreviazioni

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

Acronimo	
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
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute;
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smartcard, ma con superiori caratteristiche di memoria e di performance;
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Incaricato alla Registrazione
ISO	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione
ITU	International Telecommunication Union: fondata nel 1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
IUT	Identificativo Univoco del Titolare: è un codice associato al Soggetto che lo identifica univocamente presso la CA; il Soggetto ha codici diversi per ogni certificato in suo possesso
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati
LoA	Level of Assurance
NTR Code	National Trade Register Code
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
OTP	OneTime Password
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Soggetto per accedere alle funzioni del dispositivo stesso

Acronimo	
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse, processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto
RA	Registration Authority – Autorità di Registrazione
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
RSA	Deriva dalle iniziali degli inventori dell'algoritmo: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SPID	Sistema Pubblico di Identità Digitale
SSCD - QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una firma elettronica Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X.500	Standard ITU-T per i servizi LDAP e directory
X.509	Standard ITU-T per le PKI

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Archiviazione

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

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del manuale operativo

Il presente Manuale Operativo, 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

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

2.2.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: ldap://ldap.infocert.it o con protocollo http all'indirizzo http://crl.infocert.it. Tale accesso può essere effettuato tramite i software messi a disposizione dalla CA e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP e/o HTTP.

La CA potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

2.3 Periodo o frequenza di pubblicazione

2.3.1 Frequenza di pubblicazione del manuale operativo

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

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

Le CRLs vengono pubblicate ogni ora.

2.4 Controllo degli accessi agli archivi pubblici

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

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

Il soggetto nel certificato è identificato con l'attributo Distinguished Name (DN) che, quindi, deve essere valorizzato e conforme allo standard X.500. I certificati vengono emessi secondo gli standard ETSI per l'emissione dei certificati qualificati e secondo le indicazioni presenti nel DPCM [5].

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

Non è facoltà del Soggetto richiedere alla CA che il certificato riporti uno pseudonimo in luogo dei propri dati reali.

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert si attiene allo standard X.500.

3.1.5 Univocità dei nomi

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

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

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

3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

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

La CA non fa verifiche sull'utilizzo di marchi, e può rifiutarsi di generare o può richiedere di

revocare un certificato coinvolto in una disputa.

3.2 Convalida iniziale dell'identità

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

N/A

3.2.3 Identificazione della persona fisica

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

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
1 LiveID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione • Pubblico Ufficiale • Datore di Lavoro per la identificazione dei propri dipendenti, collaboratori, agenti	N/A

Modalità	Soggetti abilitati a eseguire l'identificazione	Strumenti di autenticazione a supporto della fase di identificazione
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 • In Italia, soggetti destinatari degli obblighi Antiriciclaggio ai sensi del D.Lgs 231/2007 e smi, Capo III [6]	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 dispositivo CNS o TS-CNS in corso di validità • Utilizzo di un dispositivo CIE in corso di validità • Identificazione tramite le credenziali di strong authentication rilasciate per l'emissione di un precedente certificato OneShot[1].
5 VideoID	• Certification Authority (CA) • Registration Authority (RA) • Incaricato alla Registrazione	N/A

3.2.3.1 Riconoscimento effettuato secondo la modalità 1 - LiveID

La modalità di identificazione **LiveID** prevede un incontro di persona tra il Soggetto, che deve aver compiuto 18 anni di età, e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti d'identificazione in corso di validità[2]. Il Soggetto deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato ad eseguire il riconoscimento. I soggetti privi di codice fiscale italiano devono esibire il documento contenente il TIN[3] o, in mancanza, un analogo codice

[1] Modalità applicabile solamente per il rilascio di certificati OneShot.

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

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

[3] Tax Identification Number, è il numero di identificazione nazionale assegnato dai paesi della Unione Europea ai propri cittadini, con finalità di identificazione nel servizio fiscale nazionale.

identificativo tratto da un documento di identità valido, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. In mancanza di tale codice identificativo potrà essere utilizzato il numero del passaporto.
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, previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte della Autorità Emittenti, nonché specifica formazione[4].
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.
L'identificazione già eseguita dal datore di lavoro, ai fini della stipula del contratto di lavoro, è considerata valida dalla CA in conformità con la seguente modalità di riconoscimento, previa verifica delle procedure operative di identificazione e di autenticazione. Analogamente, è considerata valida in conformità alla seguente modalità di riconoscimento, l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia, previa verifica delle procedure operative di 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[5]. 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 esecuzione.
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. [6], a norma del quale i clienti sono tenuti a fornire - sotto la propria responsabilità - tutte le informazioni necessarie e aggiornate per consentire ai Soggetti destinatari degli Obblighi elencati nel Capo III della predetta norma, di adempiere agli obblighi di identificazione della clientela. I soggetti destinatari degli obblighi acquisiscono i dati in base alle procedure definite in autonomia nel rispetto di quanto previsto dal Titolo II e dal Titolo III del D.Lgs. 231/2007 e s.m.i., ovvero alle analoghe procedure adottate

[4] Tali casi saranno comunicati all'Autorità di Vigilanza.

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

secondo le norme antiriciclaggio vigenti alla data del riconoscimento (anche se in epoca anteriore al presente Manuale).
Questa modalità di identificazione prevede il conferimento, da parte della CA, di un mandato con rappresentanza al soggetto destinatario degli obblighi, che agisce quindi da RA. I dati identificativi del Soggetto raccolti all'atto del riconoscimento sono conservati dalla CA di norma in modalità elettronica e possono essere conservati anche in modalità analogica.

3.2.3.3 Riconoscimento effettuato secondo la modalità 3 - SignID

Nella **modalità 3 SignID** la CA InfoCert si basa sul riconoscimento già effettuato da un'altra CA che emette certificati qualificati**.** Il Soggetto è già in possesso di un certificato 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.

3.2.3.4 Riconoscimento effettuato secondo la modalità 4 - AUTID

Nella **modalità 4 AutID** la CA si basa sul riconoscimento già effettuato alternativamente dai seguenti soggetti:

- Ente Emettitore di CNS (Carta nazionale dei Servizi) o TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi);
- Comune che ha rilasciato la CIE (Carta di Identità Elettronica);
- Certification Authority InfoCert, nell'ambito di una precedente emissione del certificato OneShot.

Il Soggetto deve essere quindi in possesso di un dispositivo sicuro con un certificato CIE o CNS ancora in corso di validità.
Per la sola emissione di certificati OneShot, InfoCert può basarsi sul riconoscimento già effettuato in occasione dell'emissione di un primo certificato OneShot. Il Soggetto, già in possesso delle credenziali di strong authentication fornite dalla CA in occasione della prima emissione, si autentica al portale della CA o della RA e richiede l'emissione di un nuovo certificato, confermando o aggiornando i dati di registrazione.
I dati di registrazione sono conservati, in questi casi, esclusivamente in formato elettronico.

3.2.3.5 Riconoscimento effettuato secondo la modalità 5 - VideoID

Nella **modalità 5 VideoID** è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphone, tablet, etc.), una webcam e un sistema audio funzionante.
L'Incaricato alla Registrazione verifica l'identità del Soggetto tramite il riscontro con uno o più documenti di riconoscimento in corso di validità, purché muniti di fotografia recente e riconoscibile.
Per ragioni di sicurezza e procedure anti-frode, il tipo di documenti accettati da questa modalità è limitato ai documenti di identità maggiormente diffusi (come ad esempio la carta di identità, la patente, il passaporto).
Le RA operanti all'estero, o che comunque identificano Soggetti residenti all'estero, possono essere autorizzati 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[6].
È facoltà del Richiedente, della RA o dell'Incaricato alla Registrazione escludere l'ammissibilità del documento utilizzato dal Soggetto se ritenuto carente delle caratteristiche elencate. I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

3.2.4 Identificazione della persona giuridica

N/A

3.2.5 Informazioni del Soggetto o del Richiedente non verificate

N/A

3.2.6 Validazione dell'autorità

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

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

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

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.
Non è possibile eseguire il rinnovo del certificato.

3.4 Identificazione e autenticazione per le richieste di revoca o sospensione

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

3.4.1 Richiesta da parte del Soggetto

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

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

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

[6] Tali casi saranno comunicati all'Autorità di Vigilanza.

3.4.2 Richiesta da parte del Richiedente

Il Richiedente che richiede la revoca o sospensione del certificato del Soggetto si autentica ai portali messi a disposizione della CA, anche mediante servizi applicativi, e opera secondo le modalità descritte nella documentazione contrattuale.

4 OPERATIVITÀ

4.1 Richiesta del certificato

4.1.1 Chi può richiedere un certificato

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

- Il Soggetto
  - rivolgendosi direttamente alla CA al sito www.firma.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 stipulando un accordo commerciale con la CA
  - rivolgendosi a una Registration Authority
  - sottoscrivendo il mandato con rappresentanza con la CA e diventando Registration Authority

4.1.2 Processo di registrazione e responsabilità

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

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

4.2 Elaborazione della richiesta

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

- prendere visione del presente Manuale Operativo, della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel paragrafo 3.2.3;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

4.2.1 Informazioni che il Soggetto deve fornire

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

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

4.2.2 Esecuzione delle funzioni di identificazione e autenticazione

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

4.2.3 Approvazione o rifiuto della richiesta del certificato

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

4.2.4 Tempo massimo per l'elaborazione della richiesta del certificato

Il tempo che intercorre dal momento della richiesta di registrazione al momento di emissione del certificato dipende dalla modalità di richiesta prescelta dal Soggetto (o Richiedente) e dalla eventuale necessità di raccogliere ulteriori informazioni.

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 remota (HSM)

Il Soggetto o il Richiedente accedono in modalità sicura ai servizi o alle applicazioni messe a disposizione alla RA dalla CA.

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

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

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

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. Nei casi in cui sia prevista la notifica da parte della CA al Soggetto, l'informazione può essere condivida anche con il Richiedente.

4.3.3 Attivazione

Il Soggetto attraverso i portali della CA o della RA, 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.

4.4 Accettazione del certificato

4.4.1 Comportamenti concludenti di accettazione del certificato

N/A

4.4.2 Pubblicazione del certificato da parte della Certification Authority

Al buon esito della procedura di certificazione, il certificato sarà inserito nel registro di riferimento

dei certificati e non sarà reso pubblico.

4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato

N/A

4.5 Uso della coppia di chiavi e del certificato

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

Il Soggetto deve custodire in maniera sicura gli strumenti e/o i codici di autenticazione per la firma remota; deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente darli 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 nell'ambito del dominio informatico definito dal contratto e per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.
Non deve apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato e non deve apporre firme elettroniche avvalendosi di certificato emesso da CA revocata.

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

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

4.5.3 Limiti d'uso e di valore

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

1.3.76.36.1.1.23	**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.**
1.3.76.36.1.1.25	"L'utilizzo del certificato è limitato ai rapporti con" seguito dall'indicazione del nome del soggetto con cui il certificato può essere utilizzato. "The certificate may be used only for relations with the" followed by the name of the subject with which the certificate can be used.

Inoltre, i certificati disciplinati dal presente Manuale sono 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 cui afferisce lo specifico dominio. I documenti informatici possono essere inerenti a rapporti tra lo stesso Richiedente e il Soggetto, oppure essere documenti di terze parti, sempre collegati al rapporto tra Richiedente e Soggetto.

Nel certificato LongTerm può quindi essere 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.

Per tutti i certificati emessi in forza del presente Manuale Operativo, è facoltà del Soggetto o del Richiedente richiedere alla Certification Authority l'inserimento nel certificato di limiti d'uso personalizzati (max 200 caratteri), o di limiti di valore che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. I valori devono essere espressi come numeri interi positivi, senza indicazione di cifre decimali. La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dalla CA per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza. La CA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

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

4.6 Rinnovo del certificato

4.6.1 Motivi per il rinnovo

Non è previsto il rinnovo dei certificati emessi in forza del presente Manuale Operativo.

4.6.2 Chi può richiedere il rinnovo

N/A

4.6.3 Elaborazione della richiesta di rinnovo del certificato

N/A

4.7 Riemissione del certificato

N/A

4.8 Modifica del certificato

N/A

4.9 Revoca e sospensione del certificato

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

4.9.1 Motivi per la revoca

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

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
   - sia venuta meno la segretezza della chiave o del suo codice d'attivazione oppure sia stato compromesso o smarrito il dispositivo OTP;
   - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave.
2. si verifica un cambiamento dei dati del Soggetto presenti nel certificato tale da rendere detti dati non più corretti e/o veritieri;
3. termina il rapporto tra il Soggetto e la CA, ovvero tra il Richiedente e la CA;
4. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

4.9.2 Chi può richiedere la revoca

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

4.9.3 Procedure per richiedere la revoca

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

4.9.3.1 Revoca richiesta dal Soggetto

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

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

4.9.3.2 Revoca richiesta dal Richiedente

Il Richiedente può richiedere la revoca del certificato del Soggetto autenticandosi ai sistemi messi a disposizione dalla CA, anche mediante servizi applicativi, operando secondo le modalità descritte nella documentazione contrattuale.

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

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

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

4.9.3.3 Revoca su iniziativa della Certification Authority

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

La CA, qualora il contratto relativo al certificato oggetto della revoca lo preveda, provvederà a comunicare l'avvenuta revoca anche al Richiedente.

4.9.4 Periodo di grazia della richiesta di revoca

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

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

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

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

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

4.9.8 Latenza massima della CRL

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

4.9.9 Requisiti servizi online di verifica

Vd appendice B

4.9.10 Altre forme di revoca

n/a

4.9.11 Requisiti specifici rekey in caso di compromissione

n/a

4.9.12 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 X 7.

4.9.13 Motivi per la sospensione

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

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

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

4.9.14 Chi può richiedere la sospensione

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

4.9.15 Procedure per richiedere la sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda del soggetto che la pone in essere. La sospensione ha sempre una durata limitata nel tempo. La sospensione termina alle ore 24:00:00 dell'ultimo giorno del periodo richiesto.

4.9.15.1 Sospensione richiesta dal Soggetto

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

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

La CA, qualora il contratto relativo al certificato oggetto della sospensione lo preveda, provvederà a comunicare l'avvenuta sospensione anche al Richiedente.

4.9.15.2 Sospensione richiesta dal Richiedente

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.

Il Richiedente può altresì 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 e alternative per la richiesta di sospensione da parte del Richiedente o del Terzo Interessato potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo e la CA.

4.9.15.3 Sospensione su iniziativa della CA

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

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

È possibile richiedere la riattivazione del certificato prima della data del termine di sospensione inviando il modulo firmato, che si trova sul sito InfoCert accompagnato da un documento di identità. Può essere inviato via PEC o FAX.

4.10 Servizi riguardanti lo stato del certificato

4.10.1 Caratteristiche operative

Le informazioni sullo stato dei certificati sono disponibili tramite CRL e servizio OCSP. Il numero di

serie di un certificato revocato rimane in CRL anche dopo la fine della validità del certificato ed almeno sino alla scadenza del certificato di CA.
Le informazioni fornite dal servizio OCSP per i certificati sono aggiornate all'ultima CRL pubblicata.

4.10.2 Disponibilità del servizio

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

4.10.3 Caratteristiche opzionali

4.11 Disdetta dai servizi della CA

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

4.12 Deposito presso terzi e recovery della chiave

N/A

5 MISURE DI SICUREZZA E CONTROLLI

Il TSP 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 la CA gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

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

Un estratto della politica di sicurezza InfoCert è disponibile facendone richiesta alla casella PEC infocert@legalmail.it.

5.1 Sicurezza fisica

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

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

5.1.1 Posizione e costruzione della struttura

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

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

Figura 1 - ubicazione Data Center InfoCert e sito della Disaster Recovery

5.1.2 Accesso fisico

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

5.1.3 Impianto elettrico e di climatizzazione

Il sito che ospita il Data Center InfoCert su Padova, pur non essendo certificato, ha le caratteristiche di un Data Center di tier 3.

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

L'infrastruttura preposta all'alimentazione include:

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

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

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

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

5.1.4 Prevenzione e protezione contro gli allagamenti

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

5.1.5 Prevenzione e protezione contro gli incendi

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

5.1.6 Supporti di memorizzazione

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

5.1.7 Smaltimento dei rifiuti

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

5.1.8 Off-site backup

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

5.2 Controlli procedurali

5.2.1 Ruoli chiave

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

5.3 Controllo del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

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

5.3.2 Procedure di controllo delle esperienze pregresse

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

5.3.3 Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, è previsto di affidare la gestione

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

5.3.4 Frequenza di aggiornamento della formazione

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

- Incontro con la Direzione 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 e reso pubblico.

5.3.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede viene regolata attraverso un piano di turnazione che viene predisposto dal responsabile di unità organizzativa mensilmente, con un anticipo di almeno 10 giorni. Ogni turno ha una durata di 8 ore lavorative.
Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicendare nel lavoro a turni il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.
Non sono previsti turni di presenza in sede notturni. I turni di presenza in sede avvengono su una fascia oraria dalle ore 07:00 alle ore 21:00 dal lunedì al venerdì e dalle 07:00 alle 12:00 il sabato.

5.3.6 Sanzioni per azioni non autorizzate

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

5.3.7 Controlli sul personale non dipendente

N/A

5.3.8 Documentazione che il personale deve fornire

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

non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette InfoCert.

5.4 Gestione del giornale di controllo

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

5.4.1 Tipi di eventi memorizzati

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

5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo

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

5.4.3 Periodo di conservazione del giornale di controllo

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

5.4.4 Protezione del giornale di controllo

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

5.4.5 Procedure di backup del giornale di controllo

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

5.4.6 Sistema di memorizzazione del giornale di controllo

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

5.5.2 Protezione dei verbali

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

5.5.3 Procedure di backup dei verbali

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

5.5.4 Requisiti per la marcatura temporale dei verbali

N/A

5.5.5 Sistema di memorizzazione degli archivi

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

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

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

5.6 Sostituzione della chiave privata della CA

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

5.7 Compromissione della chiave privata della CA e disaster recovery

5.7.1 Procedure per la gestione degli incidenti

La CA ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27000. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente e inviato al Sistema di Conservazione InfoCert; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirante a eliminare le cause che possono aver dato luogo all'incidente, se sotto il controllo di InfoCert in conformità all'articolo 19 del regolamento.

5.7.2 Corruzione delle macchine, del software o dei dati

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

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

5.7.3 Procedure in caso di compromissione della chiave privata della CA

La compromissione della chiave di certificazione è considerato un evento particolarmente critico, in quanto invaliderebbe i certificati emessi firmati con tale chiave. Vi è quindi una particolare attenzione alla protezione della chiave di certificazione e a tutte le attività di sviluppo e manutenzione del sistema che possono avere impatto sulla stessa.
InfoCert ha descritto la procedura da seguire in caso di compromissione della chiave, nell'ambito del SGSI certificato ISO 27000, dandone evidenza anche ad AgID e al CAB.

5.7.4 Erogazione dei servizi di CA in caso di disastri

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

5.8 Cessazione del servizio della CA o della RA

Nel caso di cessazione dell'attività di certificazione, InfoCert comunicherà questa intenzione

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

6 CONTROLLI DI SICUREZZA TECNOLOGICA

6.1 Installazione e generazione della coppia di chiavi di certificazione

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

Le chiavi sono generate solamente da personale esplicitamente incaricato di tale funzione. La generazione delle chiavi e della firma avviene all'interno di moduli crittografici dedicati e certificati come richiesto dalla normativa vigente.

La protezione delle chiavi private della CA viene svolta dal modulo crittografico di generazione ed utilizzo della chiave stessa. La chiave privata può essere generata solo con la presenza contemporanea di due operatori incaricati della generazione. La generazione delle chiavi avviene in presenza del responsabile del servizio.

Le chiavi private della CA vengono duplicate, al solo fine del loro ripristino in seguito alla rottura del dispositivo sicuro di firma, secondo una procedura controllata che prevede la suddivisione della chiave e del contesto su più dispositivi come previsto dai criteri di sicurezza del dispositivo HSM.

Il modulo di crittografia utilizzato per la generazione delle chiavi e per la firma ha requisiti tali da assicurare:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equi probabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo tale che non sia possibile l'intercettazione del valore della chiave privata utilizzata.

6.1.1 Generazione della coppia di chiavi del Soggetto

Le chiavi asimmetriche sono generate all'interno di un Dispositivo Sicuro per la Creazione della Firma SSCD ovvero QSCD 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. La CA procederà a eseguire audit periodici.

6.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico, sia esso un SSCD o un QSCD che, per i

certificati oggetto del presente Manuale Operativo, è sempre un HSM. Con la consegna al Soggetto dei codici o degli eventuali dispositivi di autenticazione previsti, questi entra in pieno possesso della chiave privata, che può utilizzare unicamente attraverso l'uso del PIN, di cui ha conoscenza esclusiva e che di norma provvede a scegliere in autonomia al momento della iscrizione.
In caso di processo di registrazione svolto in presenza del Soggetto, gli eventuali dispositivi di autenticazione sono consegnati non appena sono generate le chiavi.
In caso di processo di registrazione svolto non in presenza del Soggetto, gli eventuali dispositivi di autenticazione sono consegnati secondo le modalità condivise nel contratto, avendo sempre cura che i dispositivi e le informazioni per l'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

La chiave pubblica della CA è contenuta nel certificato della CA. Il certificato della CA è reso disponibile agli utenti in maniera da impedire possibilità di sostituzione.

6.1.5 Algoritmo e lunghezza delle chiavi

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

6.1.6 Controlli di qualità e generazione della chiave pubblica

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

6.1.7 Scopo di utilizzo della chiave

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

6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

6.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da 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 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in Europa.

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

6.2.2 Controllo di più persone della chiave privata di CA

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

6.2.3 Deposito presso terzi della chiave privata di CA

N/A

6.2.4 Backup della chiave privata di CA

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

6.2.5 Archiviazione della chiave privata di CA

N/A

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

N/A

6.2.7 Memorizzazione della chiave privata su modulo crittografico

La chiave di certificazione viene generata e memorizzata in un'area protetta del dispositivo crittografico 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 legale rappresentante della persona giuridica è responsabile di proteggere la propria chiave privata con una password robusta per prevenire l'utilizzo non autorizzato. Per attivare la chiave privata, il Soggetto deve autenticarsi.

6.2.9 Metodo di disattivazione della chiave privata

N/A

6.2.10 Metodo per distruggere la chiave privata della CA

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

6.2.11 Classificazione dei moduli crittografici

N/A

6.3 Altri aspetti della gestione delle chiavi

N/A

6.3.1 Archiviazione della chiave pubblica

N/A

6.3.2 Periodo di validità del certificato e della coppia di chiavi

Il periodo di validità del certificato è determinato sulla base:

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

L'intervallo di validità del certificato è espresso al suo interno nella modalità indicata al paragrafo § 3.3.1.

Attualmente il certificato della CA ha una durata di 16 anni, i certificati emessi a persona fisica o giuridica hanno validità non superiore ai 3 anni.

6.4 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.2 e 6.3.

6.5 Controlli sulla sicurezza informatica

6.5.1 Requisiti di sicurezza specifici dei computer

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

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

6.6 Operatività sui sistemi di controllo

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.
InfoCert è certificata ISO/IEC 27001:2005 da marzo 2011 per le attività EA:33-35. Nel marzo 2015 è stata certificata per la nuova versione dello standard ISO/IEC 27001:2013.

Nel SGSI sono previsti procedure e controlli per:

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

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

6.7 Controlli di sicurezza della rete

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

amministratori/operatori.

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

6.8 Controlli di sicurezza della rete

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

7 FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP

7.1 Formato del certificato

Nel certificato compaiono le informazioni indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme al Regolamento eiDAS e alla Deliberazione CNIPA [9]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.
InfoCert utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.
In 0 il tracciato dei certificati di root e dei soggetti, siano essi persone fisiche o giuridiche.

7.1.1 Numero di versione

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

7.1.2 Estensioni del certificato

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

7.1.3 OID dell'algoritmo di firma

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

7.1.4 Forme di nomi

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

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2.

7.2 Formato della CRL

Per formare le liste di revoca CRLs, InfoCert utilizza il profilo RFC5280 "Internet X.509 Public Key Infrastructure Certificate R-evocation 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 C.

7.3 Formato dell'OCSP

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

7.3.1 Numero di versione

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

7.3.2 Estensioni dell'OCSP

Per le estensioni dell'OCSP si veda Appendice C.

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.
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.

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

8.4 Aspetti oggetto di valutazione

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

8.5 Azioni in caso di non conformità

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

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

9.1.1 Tariffe per il rilascio dei certificati

Di norma, i costi per l'emissione del certificato sono sostenuti dal Richiedente e non dal Soggetto, in base a tariffe definite dal contratto di servizi tra il Richiedente e InfoCert. Il contratto con il Soggetto, comunque, può prevedere specifiche tariffe anche per quanto riguarda il Soggetto.

9.1.2 Tariffe per l'accesso ai certificati

N/A

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

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

9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili presso 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 Richiedenti prevedendo tariffe specifiche.

9.1.5 Politiche per il rimborso

Qualora il contratto non stabilisca diversamente, il Soggetto consumatore di norma rinuncia al diritto di recedere dal contratto entro il termine di 14 giorni a decorrere dalla data di conclusione del contratto.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

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

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

9.2.2 Altre attività

N/A

9.2.3 Garanzia o copertura assicurativa per i soggetti finali

Si veda il paragrafo 9.2.1.

9.3 Confidenzialità delle informazioni di business

9.3.1 Ambito di applicazione delle informazioni confidenziali

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

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

N/A

9.3.3 Responsabilità di protezione delle informazioni confidenziali

N/A

9.4 Privacy

Le informazioni relative al Soggetto e al Richiedente di cui la CA viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico {chiave pubblica, certificato (se richiesto dal Soggetto), date di revoca e di sospensione del certificato}. In particolare i dati personali vengono trattati da InfoCert in conformità a quanto indicato nel Decreto Legislativo 30 giugno 2003, n. 196 [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 Responsabilità di protezione dei dati personali

La Responsabilità è formalmente assegnata a:

Alfredo Esposito
Responsabile Sicurezza & Compliance e del Trattamento Dati personali
InfoCert S.p.A.
Sede Operativa
Via Marco e Marcelliano 45
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. Informative specifiche possono essere presenti sul sito del Richiedente, che raccoglie il consenso al trattamento per conto di InfoCert. Prima di eseguire ogni trattamento di dati personali, InfoCert procede a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge [4].

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

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

9.4.7 Altri motivi di divulgazione

Non previsti.

9.5 Proprietà intellettuale

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

9.6 Rappresentanza e garanzie

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

9.7 Limitazione di garanzia

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

9.8 Limitazione di responsabilità

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

9.9 Indennizzi

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

9.10 Termine e risoluzione

9.10.1 Termine

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

9.10.2 Risoluzione

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

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata revoca del certificato.

9.11 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1.

9.12 Revisione del Manuale Operativo

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

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

numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo Manuale Operativo verrà prontamente comunicata alle RA.
Se i cambiamenti sono rilevanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

Versione/Release n°:	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 Corretta definizione di one-shot Generalizzata la revoca/sospensione anche per certificato oneshot
Motivazioni:	Accreditamento "Infocert Firma Qualificata 2"

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 § 4.9.12 descritta la modalità di riattivazione della sospensione § 4.5.3 specificato limite d'uso per certificato OneShot
Motivazioni:	-

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

9.12.1 Storia delle revisioni

Essendo la prima release del documento, non è ancora presente una storia delle revisioni.

9.12.2 Procedure di revisione

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le

revisioni sono apportate di concerto con il Responsabile del Servizio di Certificazione, il Responsabile della Sicurezza, il Responsabile della Privacy, l'Ufficio Legale e l'Area di Consulenza e approvate dal management.

9.12.3 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del TSP (indirizzo: http://www.firma.infocert.it/doc/manuali.htm);
- in formato cartaceo può essere richiesto al contatto per gli utenti finali di cui al § 1.5.1.;
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;
- in formato elettronico sul sito web della Registration Authority e/o del Richiedente.

9.12.4 Casi nei quali l'OID deve cambiare

N/A

9.13 Risoluzione delle controversie

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

9.14 Foro competente

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

9.15 Legge applicabile

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

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

[1] Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (referenziato anche come *Regolamento eIDAS*).

[2] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (referenziato anche come *CAD*) e ss.m.ii.

[3] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e ss.mm.ii.

[4] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii.

[5] DPCM 22 febbraio 2013 (GU n.117 del 21-5-2013) - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.
[6] D.Lgs. 21 novembre 2007, n. 231 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e ss.mm.ii.
[7] Decreto Legislativo 6 settembre 2005, n.206 e ss.mm.ii - Codice del Consumo.
[8] Provvedimento Garante per la protezione dei dati personali 26 marzo 2003 [1053753].
[9] Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determine successive.

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza[7], nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].

9.16 Disposizioni varie

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

9.17 Altre disposizioni

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

Servizio	Orario
Accesso all'archivio pubblico dei certificati (comprende i certificati e le CRL).	Dalle 0:00 alle 24:00 7 giorni su 7
Revoca e sospensione dei certificati.	Dalle 0:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione, pubblicazione, rinnovo[8].	Dalle 8:00 alle 18:00 dal lunedì al venerdì esclusi i festivi Dalle 8:00 alle 13:00 il sabato
Richiesta e/o verifica di marca temporale.	24hx7gg (disponibilità minima 95%)

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

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

Appendice A **Root CA**

```
  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
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 {
  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
         :     }
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 ]
         :   }
```

Appendice B Certificati

Certificato qualificato persona fisica con identificatori e chiavi semantiche su QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)*** *as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "***VATIT-***TaxIdentificationNumber", "***NTRIT-***IdentifierNationalTradeRegister")*
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)*** *as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "***TINIT-***Codicefiscale", "***PASIT-***PassportNumber", "***IDCIT-***IdentityCardNumber")*
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	

http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.64 • 1.3.76.36.1.1.65
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE (optional)*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1) *(mandatory)* id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(optional)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
(*): the pseudonym attribute shall not be present if the givenName and surname attributes are present	
(**): if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present	
(***): when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier	
NB: xx = partitioned revocation list progressive numbering	

Certificato qualificato persona fisica SENZA identificatori e chiavi semantiche su QSCD emesso dalla CA "InfoCert Qualified Electronic Signature CA 3"

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	

Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.64 (firma qualificata one-shot) • 1.3.76.36.1.1.65 (firma qualificata remota)
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE (optional)*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
NB: xx = partitioned revocation list progressive numbering	

Certificato qualificato persona fisica SENZA identificatori e chiavi semantiche su QSCD emesso dalla CA "InfoCert Qualified Electronic Signature CA 3"

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	INFOCERT SPA
Organizational Unit Name:	Certificatore Accreditato
serialNumber	07945211006
Common Name:	InfoCert Firma Qualificata 2
VALIDITY:	da un ora a tre anni
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/crls/firma2/CRLxx.crl	
Uniform Resource ID2:	

Field	Value
URI	= ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20Qualificata%202%20CRL05,ou%3DCertificatore%20Accreditato,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.sc.infocert.it/
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca2/firma2/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.34 (firma qualificata one-shot) • 1.3.76.36.1.1.35 (firma qualificata remota)
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

Field	Value
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE (optional)*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
NB: xx = partitioned revocation list progressive numbering	

Appendice C 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
Issuing Distribution Point	Identifica il punto di distribuzione delle CRL e lo scopo: indica se la CRL è generata solo per certificati di CA, solo certificati di attributo o del soggetto
Invalidity Date	Data in formato UTC che indica la data da cui si ritiene che il certificate sia invalido

La richiesta OCSP contiene i seguenti campi:

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

La risposta OCSP contiene i seguenti campi:

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

Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

La richiesta OCSP contiene 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 una requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in una responseExtensions.

La risposta OCSP contiene 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 una requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in una responseExtensions.

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

InfoCert mette a disposizione un prodotto (denominato "Dike") scaricabile gratuitamente dai Soggetti 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 specifici atti di implementazione del Regolamento.

Gli ambienti in cui Dike 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 Dike 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.

I 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.

Di norma, i documenti firmati utilizzando i certificati emessi in virtù del presente CPS, in formato PAdES, sono verificabili con lo strumento Adobe Reader®.

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.