Manuale Operativo

Certificate Policy
Certificate Practice Statement
per
certificati di autenticazione siti WEB

CODICE DOCUMENTO	ICERT-INDI-MOWS
VERSIONE	3.2
DATA	11/02/2020

InfoCert
TINEXTA GROUP

Sommario

INDICE DELLE FIGURE

1 Introduzione

1.1 Quadro generale

Un certificato lega la chiave pubblica ad un insieme di informazioni che identificano il soggetto o il dispositivo/sistema che possiede la corrispondente chiave privata: tale persona fisica o giuridica e/o dispositivo/sistema è il **Soggetto** del certificato. Il certificato è usato da altri utenti per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma elettronica qualificata apposta ad un documento o ad un challenge. 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 certificazione di siti web e di applicazioni Client. Il manuale contiene le politiche e le pratiche seguite da InfoCert nel processo di controllo delle richieste, identificazione dei richiedenti ed emissione dei certificati, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, e in generale di tutto ciò che rende affidabile un certificato qualificato e non di siti web e applicazioni Client, in conformità con la vigente normativa in materia di servizi fiduciari ed i requisiti definiti nei documenti CAB Forum Guidelines (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 1.6.7 del 19 Dicembre 2019 referenziato nel seguito come "Baseline Requirements [BR]" e Guidelines for Extended Validation Certificates 1.7.1 del 19 Dicembre 2019 referenziato nel seguito come "EV Guidelines [EVG]").

Se ci fosse qualche inconsistenza tra questo documento e i requisiti elencati nei documenti CAB Forum elencati sopra, questi ultimi fanno fede.

Pubblicando il presente 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 del presente Manuale Operativo si basa sulle norme vigenti alla data di emissione e recepisce le raccomandazioni del documento "Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003.

Il presente Manuale Operativo contiene altresì le politiche e le pratiche seguite da InfoCert nel processo di controllo delle richieste, identificazione dei richiedenti ed emissione dei certificati per autenticazione siti web di cui all'art 34 Regolamento Delegato (UE) 2018/389 [9], di attuazione della Direttiva (UE) 2015/2366 (PSD2) [8], in conformità con i requisiti definiti dallo standard ETSI TS 119 495 (referenziati nel seguito come "Certificati PSD2").

1.2 Nome ed identificativo del documento

Questo documento è denominato "Prestatore di Servizi Fiduciari InfoCert – Certificazione Web Server e Client- Manuale Operativo" ed è caratterizzato dal codice documento: **ICERT-INDI-MOWS**.

La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

La versione 1.0 del presente documento è relativa alle chiavi di certificazione (root CA e subCA) generate dopo 11 dicembre 2016.

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. L'*object identifier* (OID) che identifica InfoCert è 1.3.76.36.

Il significato degli OID è il seguente:

Certificato qualificato (QWAC) per validazione del dominio e dell'organizzazione che controlla il dominio per applicazione SSL non browser (A2A) **Disponibile anche per PSD2**	1.3.76.36.1.1.45.4 conforme alle policy ETSI QCP-w **0.4.0.194112.1.4**
Certificato qualificato (QWAC) OV per validazione del dominio e dell'organizzazione che controlla il dominio (Organization Validation) **Disponibile anche per PSD2**	1.3.76.36.1.1.45.2 conforme alle policy: ETSI QCP-w-psd2 0.4.0.19495.3.1 (fino al 01/10/2019) ETSI QCP-w **0.4.0.194112.1.4** (dal 01/10/2019) CAbForum 2.23.140.1.2.2
Certificato qualificato (QWAC) EV per validazione del dominio e dell'entità legale che controlla il dominio (Extended Validation)	1.3.76.36.1.1.45.3 conforme alle policy ETSI QCP-w **0.4.0.194112.1.4** CabForum 2.23.140.1.1
Certificato OV per validazione del dominio e dell'organizzazione che controlla il dominio (Organization Validation)	1.3.76.36.1.1.19.2 conforme alle policy ETSI OVCP **0.4.0.2042.1.7** CabForum 2.23.140.1.2.2
Certificato OV per validazione dell'organizzazione (Organization Validation)	1.3.76.36.1.1.19.5 conforme alle policy ETSI **OVCP 0.4.0.2042.1.7** CabForum 2.23.140.1.2.2

1.3 Partecipanti e responsabilità

1.3.1 Certification Authority – Autorità di Certificazione

La **Certification Authority** è il soggetto terzo fidato che emette i certificati digitali qualificati, firmandoli con la propria chiave privata, detta chiave di CA.

InfoCert è la Certification Authority (**CA**) che emette e revoca i certificati digitali qualificati, operando in conformità ai requisiti di CAB Forum, alle regole tecniche emanate dall'Autorità di Vigilanza e secondo quanto prescritto dal Regolamento eIDAS [1].

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

Denominazione sociale	**InfoCert – Società per azioni** **Società soggetta a direzione e coordinamento di Tinexta S.p.A.**
Sede legale	Piazza Sallustio n.9, 00187, Roma (RM)
Sede operativa	Via Marco e Marcelliano n.45, 00147, Roma (RM)
Rappresentante legale	Danilo Cattaneo In qualità di Amministratore Delegato
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 Richiedente,
- la registrazione dei dati del Soggetto,
- l'inoltro dei dati del Soggetto ai sistemi della CA,
- la raccolta della richiesta del certificato,
- la fornitura di supporto al Richiedente e alla CA nelle eventuali fasi di generazione, 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.
La CA può delegare buona parte delle attività ad una Registration Authority, tranne la validazione del dominio e la certificazione della chiave pubblica che deve essere eseguito dalla CA (con i metodi previsti).

Le RA sono attivate dalla CA a seguito di un adeguato addestramento del personale impiegato (Validation Specialist); la CA verifica la rispondenza delle procedure utilizzate a quanto stabilito dal presente Manuale.

1.3.3 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.
Nello specifico si individuano le seguenti casistiche:

- Può essere la persona fisica che ha i poteri di richiedere un certificato per il Soggetto (sistema);
- Può essere la persona giuridica che richiede un certificato per il Soggetto (sistema).

1.3.4 Soggetto

È il sistema o sito WEB per cui il Richiedente richiede il certificato. In alcuni casi viene definito anche come Titolare

1.3.5 Utente

È un sistema o persona che verifica 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 dispositivo o sistema certificato, nei contesti dove esso è utilizzato. Corrisponde a quanto descritto nei documenti del CabForum a Relying Party

1.3.6 Autorità

1.3.6.1 Agenzia per l'Italia Digitale - AgID

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

1.3.6.2 Organismo di valutazione della conformità - Conformity Assessment Body

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

1.3.6.3 Autorità nazionale competente (NCA)

In ambito PSD2[8], l'autorità nazionale di vigilanza degli intermediari finanziari è l'organismo responsabile dell'autorizzazione dei PSP di ciascun stato membro. Se l'autorizzazione è concessa, la NCA emette un numero di autorizzazione e pubblica tali informazioni nei propri registri pubblici.

1.3.6.4 Autorità bancaria europea (EBA)

L'autorità bancaria europea (**EBA**), opera per assicurare un livello di regolamentazione e di vigilanza uniforme nel settore bancario europeo. In ambito PSD2[8], vigila e si fa garante della trasparenza

dell'operato dei prestatori di servizi di pagamento (PSP) autorizzati dalle NCA competenti per ciascuno stato membro. Ha in carico lo sviluppo e la gestione del "Registro elettronico centrale", nel quale ogni NCA deve pubblicare l'elenco di nomi e le informazioni riferite ai soggetti autorizzati.

1.4 Uso del certificato

1.4.1 Usi consentiti

L'uso primario questo tipo di certificati è quello di consentire una comunicazione elettronica efficiente e sicura, garantita da una CA.

I certificati emessi dalla CA InfoCert, secondo le modalità indicate dal presente manuale operativo, sono Certificati Qualificati ai sensi dell'articolo 45 del Regolamento eIDAS "Requisiti per i certificati qualificati di autenticazione di siti web" ovvero certificati non qualificati per autenticazione siti WEB e Client ai sensi del Regolamento EIDAS.

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 (*key usage*, *extended key usage, user notice*) indicati nel certificato.

E' vietato l'utilizzo per attività illecite.

1.5 Amministrazione del Manuale Operativo

1.5.1 Organizzazione responsabile del documento

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.

1.5.2 Contatti

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: 06 54641489
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.

1.5.3 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle Policies, dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dall'Ufficio Legale e dall'Area di Consulenza e viene approvato dal management aziendale.

1.5.4 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2008.
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
CAB – Conformity Assessment Body (Organismo di valutazione della conformità)	Organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
CAR – Conformity Assessment Report (Relazione di valutazione della conformità)	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr eIDAS [1]).
autenticazione	un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica (cfr eIDAS [1])
certificato di autenticazione di siti web	Un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato (cfr eIDAS [1])
certificato qualificato di autenticazione di sito web (QWAC)	Un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV (cfr eIDAS [1])
chiave di certificazione o chiave di root	Coppia di chiavi crittografiche utilizzate dalla CA per firmare i certificati e le liste dei certificati revocati o sospesi

Termine	Definizione
chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Soggetto, mediante la quale si appone la firma elettronica qualificata sul documento informatico (cfr CAD [2]).
chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma elettronica qualificata apposta sul documento informatico dal Soggetto (cfr CAD [2]).
Convalida	Il processo di verifica e conferma della validità di una firma (cfr eIDAS [1])
CSR	Un CSR (Certificate Signing Request) è un file di testo cifrato che viene utilizzato per la richiesta di un certificato di autenticazione WEB. In questo file sono contenute tutte le informazioni che le Autorità di Certificazione (CA) utilizzano per creare il certificato.
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])
documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1])
firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (cfr eIDAS [1])
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
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])

Termine	Definizione
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
registro pubblico [Directory]	Il Registro pubblico è un archivio che contiene: ▪ tutti i certificati emessi dalla CA per i quali sia stata richiesta dal Richiedente 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
CAA	Certification Authority Authentication
CAB	Conformity Assessment Body – Organismo di valutazione della

Acronimo	
	conformità
CABForum	Certification Authority Browser Forum
CAR	Conformity Assessment Report – Relazione di valutazione della conformità
CC	Common Criteria
CIE	Carta di Identità Elettronica;
CRL	Certificate Revocation List;
CRS	Certificate Signing Request
DMZ	Demilitarized Zone
DN	Distinguished Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute;
EV	Validazione dell'organizzazione. Tipo di certificato di autenticazione WEB con verifica estesa dell'organizzazione in relazione al dominio certificato
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name (è un nome di dominio non ambiguo che specifica la posizione assoluta di un nodo all'interno della gerarchia dell'albero DNS)
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, 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;

Acronimo	
LoA	Level of Assurance
NCA	National Competent Authority
NTR Code	National Trade Register Code
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia;
OV	Validazione dell'organizzazione. Tipo di certificato di autenticazione WEB con verifica dell'organizzazione in relazione al dominio certificato o di autenticazione Client con verifica dell'organizzazione
PEC	Posta Elettronica Certificata
PEM	Privacy Enhanced Mail formato per memorizzare chiavi e certificati che rispetta RFC 7468
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Soggetto per accedere alle funzioni del dispositivo stesso;
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse, processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto
PSD2	Payment Services Directive 2
PSP	Payment Service Provider. Organizzazione che è altresì prestatore di servizi a pagamento
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority – Autorità di Registrazione
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
RSA	Deriva dalle iniziali degli inventori dell'algoritmo: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SPID	Sistema Pubblico di Identità Digitale
SSCD – QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una firma elettronica Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X509	Standard ITU-T per le PKI
X500	Standard ITU-T per i servizi LDAP e directory

1.6.3 Riferimenti

[BR]	CA/Browser Forum, "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates". Ver 1.6.7 del 19 Dicembre 2019
[EVG]	CA/Browser Forum, "Guidelines For The Issuance And Management Of Extended Validation Certificates". Ver. 1.7.1 del 19 Dicembre 2019
[RFC3647]	Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003.
[RFC5280]	Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013
[RFC6962]	Request for Comments: 6962, Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013
[PSD2]	Art 34 Regolamento Delegato (UE) 2018/389 [9], di attuazione della Direttiva (UE) 2015/2366 (PSD2) in conformità con i requisiti definiti dallo standard ETSI TS 119 495
[ETSI411-1]	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. V1.2.2
[ETSI411-2]	ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. V2.2.2
[ETSI401]	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers V2.2.1
[ETSI403]	ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers V2.2.2
[UNICEI]	UNI CEI EN ISO/IEC 17065:2012
[GDPR]	Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018
[DLGS196]	Decreto Legislativo 30 giugno 2003, n. 196
[X.509]	Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
[TP]	TSP Termination CA v. 1.3 del 08/07/2019 reperibile presso il Certificatore

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Archiviazione

Le CRLs e i manuali operativi sono pubblicati e disponibili 24 ore al giorno per 7 giorni alla settimana.
InfoCert mette a disposizione delle pagine di test per *InfoCert Organization Validation CA 3*:
https://valid.ovcf.ca3.infocert.it
https://expired.ovcf.ca3.infocert.it
https://revoked.ovcf.ca3.infocert.it

e le seguenti pagine di test per *InfoCert Organization Validation 2019 CA 3*:
https://valid.ovcf2019.ca3.infocert.it
https://expired.ovcf2019.ca3.infocert.it
https://revoked.ovcf2019.ca3.infocert.it

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del manuale operativo

Il presente Manuale Operativo è reperibile in formato elettronico presso il sito web della Certification Authority (cfr. § 1.5.2).
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. § 1.5.2).

2.2.2 Pubblicazione dei certificati

No Stipulation

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 24 ore.

2.4 Controllo degli accessi agli archivi pubblici

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

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

Il soggetto nel certificato è identificato con l'attributo Distinguished Name (DN) che, quindi, deve essere valorizzato e conforme allo standard X500. I certificati vengono generati secondo gli standard ETSI per l'emissione dei certificati qualificati e secondo le linee guida di CABForum.

I certificati SSL Wildcard includono un carattere asterisco con carattere jolly come nel nome del dominio. Prima di emettere un certificato con un carattere jolly (*) InfoCert controlla che non si trovi nella prima posizione a sinistra dopo l'estensione (ad esempio "* .com", "* .it") e rifiuterà la richiesta.

3.1.2 Necessità che il nome abbia un significato

L'attributo del certificato Subject Distinguished Name (SDN) identifica in maniera univoca e chiara il soggetto (organizzazione, device o altro oggetto) a cui è rilasciato il certificato.

3.1.3 Anonimato e pseudonimia dei richiedenti

No Stipulation

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert si attiene allo standard X500.

3.1.5 Univocità dei nomi

Nei certificati di autenticazione siti WEB è presente il nome del dominio. Questo viene controllato negli archivi gestiti da ICANN (Internet Corporation for Assigned Names and Numbers).

InfoCert applica l'unicità di ciascun nome del soggetto includendo il dominio/i nell'estensione del certificato SubjectAlternativeName.

Il commonName se presente deve contenere un dominio presente nel SubjectAlternativeName.

3.1.6 Il dominio presente Riconoscimento, autenticazione e ruolo dei marchi registrati

Il Richiedente, quando richiede un certificato alla CA garantisce di operare nel pieno rispetto delle normative nazionali e internazionali sulla proprietà intellettuale.

La CA può eseguire l'identificazione del Richiedente, utilizzando qualsiasi mezzo legale di comunicazione o indagine necessario per identificare l'Entità.

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 Richiedente al momento della richiesta di rilascio del certificato.

La procedura di identificazione comporta che il Richiedente 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.

InfoCert può rifiutare la generazione del certificato richiesto a sua unica discrezione.

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 contenuta nella richiesta di certificato apposta con la chiave privata corrispondente alla chiave pubblica da certificare.
In caso di certificati di autenticazione Client, la chiave privata puo' essere generata dalla CA stessa.

3.2.2 Autenticazione dell'identità delle organizzazioni

Ferma restando la responsabilità della CA, l'identità del Richiedente viene accertata dai soggetti abilitati a eseguire il riconoscimento.
La CA mantiene politiche e procedure interne che vengono riviste regolarmente al fine di rispettare i requisiti dei Baseline Requirements e degli Extended Validation Requirement.
I nomi dei domini inclusi in un certificato OV di siti web vengono verificati secondo quanto specificato al $ 3.2.2 dei Baseline Requirements.
Se il subject Distinguished Name di un certificato di siti web o di autenticazione Client, contiene un nome nel campo organization, la CA verifica il nome dell'organizzazione e la sua esistenza secondo quanto specificato al $ 3.2.2.1 dei Baseline Requirements tramite l'uso di basi dati governative o di terze parti o tramite comunicazioni dirette con l'ente che sovrintende la creazione e il riconoscimento di un'entità legale nel paese in cui è stabilita.

3.2.2.1 Identificazione del richiedente

L'identità del Richiedente viene accertata dai soggetti abilitati a eseguire il riconoscimento nelle stesse modalità descritte del manuale operativo INFOCERT-INDI-MO per l'emissione dei certificati di firma qualificata a persona fisica e/o giuridica.

3.2.3 Autenticazione dell'identità di una persona

No Stipulation

3.2.4 Informazioni non verificate

No Stipulation

3.2.5 Istruttoria da parte della CA

InfoCert, sulla base delle informazioni fornite dal Richiedente, procederà alle opportune verifiche dei dati comunicati: devono essere congruenti tra loro e, in caso di certificati di autenticazione siti

WEB, congruenti con quanto pubblicato in registri pubblici che registrano la proprietà dei domini Internet (per l'Italia www.nic.it).

Per le Pubbliche Amministrazioni si dovrà fare riferimento agli indici nazionali (per l'Italia www.indicepa.gov.it).

In caso di certificati PSD2, InfoCert verifica gli attributi specifici forniti dal soggetto Richiedente (numero di autorizzazione, nome e stato della NCA, ruolo del PSP) utilizzando le informazioni autentiche rese disponibili da EBA all'interno del proprio registro centrale o, eventualmente, nei registri resi disponibili dalle NCA di ciascuno stato membro.

Se la NCA nazionale ha fornito delle regole per la convalida di tali attributi, il TSP applica le regole indicate.

Viene verificato inoltre, nei casi previsti, il contenuto della CSR (certificate signing request) che, a sua volta, deve contenere informazioni congruenti con quanto indicato nel modulo di richiesta ($ 4.2.1).

Qualsiasi discrepanza rende impossibile l'emissione del certificato. InfoCert si riserva di chiedere documentazione integrativa qualora si rendesse necessario per confermare l'autenticità delle richieste ricevute.

Una volta verificate ed approvate le informazioni, ad esclusione dei certificati di autenticazione Client, InfoCert effettua il **Domain Control Validation**, ovvero il controllo che il richiedente abbia l'effettiva disponibilità del sito che sta andando a certificare.

Certificato OV	InfoCert verifica il diritto del Richiedente ad utilizzare ogni dominio di cui chiede la certificazione attraverso uno o più dei seguenti modi: - **Verifica nei registri pubblici.** - Comunicazione di un valore random ad uno dei seguenti indirizzi email del dominio oggetto di certificazione webmaster@, administrator@, admin@, hostmaster@, postmaster@ e conseguente ricezione di una risposta che identifica il medesimo valore random. - **Comunicazione di un valore random tramite e-mail, fax, sms, posta cartacea agli indirizzi indicati nei registri o in documenti ufficiali e conseguente ricezione di una risposta che identifica il medesimo valore random.** - Richiedendo una dimostrazione pratica del controllo dei siti web - **Richiedendo una dimostrazione pratica del controllo del dns dei domini in cui risiedono i siti web.** - **Telefonata ad un numero presente tra i contatti del dominio, da utilizzare solamente come modalità ulteriore di verifica e non come singola modalità.**

	InfoCert esegue le stesse verifiche di cui sopra e le verifiche previste per l'autenticazione e validazione di una persona giuridica (fare riferimento al manuale operativo InfoCert per i certificati qualificati ICERT-INDI-MO)
Certificato EV or QWAC	InfoCert verifica il diritto del Richiedente ad utilizzare ogni dominio di cui chiede la certificazione attraverso uno o più dei seguenti modi: - **Verifica nei registri pubblici.** - Comunicazione di un valore random ad uno dei seguenti indirizzi email del dominio oggetto di certificazione webmaster@, administrator@, admin@, hostmaster@, postmaster@ e conseguente ricezione di una risposta che identifica il medesimo valore random. - **Comunicazione di un valore random tramite e-mail, fax, sms, posta cartacea agli indirizzi indicati nei registri o in documenti ufficiali e conseguente ricezione di una risposta che identifica il medesimo valore random.** - Richiedendo una dimostrazione pratica del controllo dei siti web - **Richiedendo una dimostrazione pratica del controllo del dns dei domini in cui risiedono i siti web.** - Telefonata ad un numero presente tra i contatti del dominio, da utilizzare solamente come modalità ulteriore di verifica e non come singola modalità. InfoCert esegue le stesse verifiche di cui sopra e le verifiche previste per l'autenticazione e validazione di una persona giuridica (fare riferimento al manuale operativo InfoCert per i certificati qualificati ICERT-INDI-MO)

La validazione del dominio rimane valida per 2 anni per cui a fronte di altre richieste afferenti al medesimo dominio le operazioni di validazione non saranno ripetute fino allo scadere dei 2 anni.

3.2.6 Interoperabilita' da parte della CA

No Stipulation

3.3 Identificazione e autenticazione per la richiesta di rinnovo delle chiavi e dei

certificati

InfoCert non prevede il rinnovo, ma solo nuove emissioni. Infocert richiede pertanto di seguire le stesse procedure di identificazione e autenticazione descritte al par. 3 Un mese prima della scadenza del certificato invierà al Richiedente un avviso che lo informa della scadenza in questione.

3.3.1 Identificazione e autenticazione per il rinnovo delle chiavi di routine

Vedi §3.2.5

3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi dopo la revoca

Vedi §3.2.5

3.4 Identificazione e autenticazione per la richiesta di revoca

Infocert autentica tutte le richieste di revoca che devono essere firmata. La verifica del richiedente viene descritta dettagliatamente al paragrafo 4.9

4 CICLO di VITA DEL CERTIFICATO

4.1 Richiesta del certificato

4.1.1 Chi può richiedere un certificato

Il certificato può essere richiesto da una persona fisica che rappresenta la persona giuridica rivolgendosi direttamente alla CA mediante le procedure presenti sul sito www.firma.infocert.it o stipulando un accordo commerciale con la CA.

I sistemi che ospitano i Client o i siti web di cui si richiede la certificazione devono essere situati in luoghi protetti in modo tale da prevenire l'eventuale compromissione, perdita, individuazione, modifica o utilizzo non autorizzato della chiave privata del server.

Detti sistemi devono, inoltre, dare adeguate garanzie di sicurezza logica, ovvero

- essere amministrati secondo procedure documentate;
- essere protetti da firewall;
- essere opportunamente configurati;
- avere in essere un sistema di controllo che limiti l'accesso al server stesso esclusivamente agli utenti all'uopo autorizzati.

4.1.2 Processo di registrazione e responsabilità

Il processo di registrazione comprende la domanda da parte del Richiedente (attraverso modulo predefinito reperibile sul sito www.firma.infocert.it), la richiesta di certificazione della chiave pubblica corrispondente alla chiave privata che nel caso di autenticazione Client puo' essere generata dalla CA 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 Richiedente ha la responsabilità di fornire informazioni corrette e veritiere sulla propria identità, di leggere attentamente il materiale messo a disposizione dalla CA, di seguire le istruzioni della CA nell'avanzare la richiesta del certificato, tali responsabilità ricadono sul legale rappresentante o soggetto munito di apposita procura;
- La Certification Authority è il responsabile ultimo della identificazione del Richiedente e del buon esito del processo di registrazione del certificato.

4.2 Elaborazione della richiesta

Per ottenere un certificato sia qualificato che non di autenticazione siti web o di autenticazione Client, 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 CA come descritte nel paragrafo 3;

- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

Il Richiedente, individuato nel legale rappresentante o persona fisica dotata di procura, **deve fornire obbligatoriamente le seguenti informazioni:**

- Cognome e Nome del Richiedente
- Codice fiscale o analogo codice identificativo del Richiedente (TIN) per cittadini stranieri
- Estremi del documento di riconoscimento presentato per l'identificazione del Richiedente, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- e-mail per l'invio delle comunicazioni dalla CA al Richiedente;
- Nome della persona giuridica (organizzazione) che detiene il controllo dei Client o dei siti web oggetto della richiesta di certificazione;
- Partita IVA ovvero numero di Registro Imprese per organizzazioni italiane, VAT code ovvero NTR per organizzazioni straniere.

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

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

In caso di certificati di autenticazione siti WEB, il Richiedente deve inoltre fornire il modulo che trova all'indirizzo Web www.infocertssl.it, compilato e firmato digitalmente.
Deve fornire la CSR in formato PKCS#10 codificata PEM e firmata digitalmente. Nel caso in cui il CSR non fosse firmata digitalmente dal richiedente, il certificatore verifica l'autenticità della richiesta ed il relativo contenuto mediante altri canali.
Nel modulo e nella CSR devono essere esattamente indicati il nome del dominio (dei domini) per il quale (i quali) si chiede la certificazione; qualora si tratti di domini di livello oltre il secondo sarà sufficiente verificare nei suddetti archivi la presenza del dominio principale.
La CSR viene generata dal richiedente una volta creata la coppia di chiavi asimmetriche; tale file, oltre alle informazioni indicate qui di seguito, conterrà la firma del sito web generata con la chiave privata corrispondente alla chiave pubblica che si desidera certificare, in modo da fornire prova di possesso della medesima chiave privata.

Nel file CSR dovranno essere inserite almeno le seguenti informazioni negli appositi campi previsti dallo standard PKCS#10 (indicati di seguito tra parentesi):

- il nome DNS del sito (dei siti) web da certificare (in DNSName nell'estensione SubjectAlternativeName);
- deve essere presente la denominazione sociale dell'organizzazione/ente proprietario del sito (dei siti) web da certificare (nel campo Organization del subject DN);
- il codice del paese dell'organizzazione/ente proprietario del sito (dei siti) web da certificare

(nel campo Country del subject DN, es. Italia=IT);

Nel file CSR possono essere inserite le seguenti informazioni negli appositi campi previsti dallo standard PKCS#10 (indicati di seguito tra parentesi):

- il nome DNS del sito (di uno dei siti) web da certificare (nel campo Common Name del subject DN).

La lunghezza della chiave pubblica generata secondo l'algoritmo RSA e di cui si richiede la certificazione (e della corrispondente chiave privata) non deve essere inferiore a 2048 bits allo scopo di fornire adeguate garanzie di sicurezza.
La certificazione della chiave pubblica può essere effettuata per ogni tipologia di Web server presente nel mercato, utilizzando gli algoritmi crittografici ammessi dal protocollo SSL e supportati dai browser Web più diffusi.

In caso di certificati di autenticazione Client, il Richiedente deve inoltre fornire il modulo che trova all'indirizzo Web www.firma.infocert.it/documentazione/, compilato e firmato digitalmente. Per richieste multiple, puo' fornire a completamento un foglio Excel, anch'esso firmato digitalmente.
Puo' fornire la CSR in formato PKCS#10 codificata PEM e firmata digitalmente.
Nel modulo e nell'eventuale CSR devono essere esattamente indicati il nome per il quale si chiede la certificazione.
La CSR viene generata dal richiedente o dalla CA. In caso di creazione da parte del richiedente, una volta creata la coppia di chiavi asimmetriche; tale file, oltre alle informazioni indicate qui di seguito, conterrà la firma del Client generata con la chiave privata corrispondente alla chiave pubblica che si desidera certificare, in modo da fornire prova di possesso della medesima chiave privata.

Nel file CSR dovranno essere inserite almeno le seguenti informazioni negli appositi campi previsti dallo standard PKCS#10 (indicati di seguito tra parentesi):

- deve essere presente la denominazione sociale dell'organizzazione/ente proprietario del client da certificare (nel campo Organization del subject DN);
- il codice del paese dell'organizzazione/ente proprietario del client da certificare (nel campo Country del subject DN, es. Italia=IT);
- la localita' dell'organizzazione/ente proprietario del client da certificare (nel campo locality del subject DN, es. Italia=IT);
- il nome dell'organizzazione/ente proprietario del client da certificare (nel campo Common Name del subject DN)

La lunghezza della chiave pubblica generata secondo l'algoritmo RSA e di cui si richiede la certificazione (e della corrispondente chiave privata) non deve essere inferiore a 2048 bits allo scopo di fornire adeguate garanzie di sicurezza.

Il Certificatore esclude ogni responsabilità per il mancato rispetto delle condizioni di sicurezza sopra esposte.

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

4.2.1 Esecuzione delle funzioni di identificazione e autenticazione

Durante la fase di registrazione iniziale e raccolta della richiesta di registrazione e certificazione la CA o la RA identificano ogni Richiedente e verificano accuratamente le informazioni fornite secondo le modalità specificate nel presente manuale.
La CA può delegare parte delle attività della Registration Authority ad una terza parte, tranne la validazione del dominio (certificati autenticazione siti WEB) che deve essere eseguito dalla CA attraverso i metodi previsti nel presente manuale.
La validazione del dominio e dell'organizzazione vengono fatte da due diverse persone fidate.

Dall' 8 settembre 2017 InfoCert esegue anche il seguente controllo: durante il processo di convalida iniziale, controlla il DNS per l'esistenza di un record CAA per ogni dNSName nel subjectAltName (certificati autenticazione siti WEB). Se esiste un record CAA che non elenca InfoCert come CA autorizzata, InfoCert verifica che il richiedente abbia autorizzato l'emissione, nonostante il record CAA.

InfoCert inoltre controlla il certificato in base a un database interno di certificati precedentemente revocati e richieste di certificati rifiutate per identificare richieste di certificati sospette.

4.2.2 Approvazione o rifiuto della richiesta del certificato

Dopo la registrazione iniziale la CA o la RA possono rifiutare di portare a termine la generazione del certificato in caso di assenza o incompletezza di informazioni, di verifiche negative o incomplete di coerenza e consistenza delle informazioni fornite, delle verifiche anti-frode, di dubbi sull'identità del Richiedente o dei dati del Soggetto, ecc. La CA non si obbliga a fornire le ragioni dell'eventuale rifiuto di una richiesta di certificazione.

4.2.3 Tempo massimo per l'elaborazione della richiesta del certificato

Il tempo che intercorre dal momento della richiesta di registrazione al momento della generazione del certificato dipende dalla modalità di richiesta prescelta dal Richiedente e dalla eventuale necessità di raccogliere ulteriori informazioni. Non devono trascorrere più di 15 giorni dal momento in cui la CA ha identificato correttamente il Richiedente e l'eventuale persona giuridica che questi rappresenta ed ha autenticato correttamente la richiesta di certificazione al momento della generazione del certificato.

4.3 Emissione del certificato

4.3.1 Azioni della CA durante l'emissione del certificato

InfoCert genera il certificato in ambiente protetto come descritto nel quinto capitolo. Nel caso di certificati EV o OV qualificati, la generazione viene fatta attraverso procedure che prevedono l'intervento contemporaneo di due persone fidate.

4.3.2 Notifica ai richiedenti dell'avvenuta generazione del certificato

Una volta generato, il certificato viene inviato al Richiedente nelle modalità concordate.

4.4 Accettazione del certificato

4.4.1 Comportamenti concludenti di accettazione del certificato

Il richiedente è l'unico responsabile dell'installazione del certificato sui propri software.

4.4.2 Pubblicazione del certificato da parte della Certification Authority

No Stipulation

4.4.3 Notifica ad altri soggetti

Secondo la specifica RFC 6962, i pre-certificate di autenticazione Web sono sottomessi a:

- due diversi Certificate Transparency (CT) log per i certificati di durata un anno
- tre diversi Certificate Transparency (CT) log per i certificati di durata un anno

secondo la specifica RFC 6962.

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 proteggere la chiave privata da accessi non autorizzati o altri utilizzi fraudolenti. Deve garantire la protezione della segretezza e la conservazione del codice di emergenza necessario alla sospensione del certificato, deve utilizzare il certificato per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.
Non deve utilizzare chiavi private per le quali sia stato revocato o sospeso il certificato ovvero avvalendosi di certificato generato da una CA che sia stata revocata.

4.5.2 Uso della chiave pubblica e del certificato da parte degli utilizzatori

Ogni utilizzatore (utente finale) deve conoscere l'ambito di utilizzo del certificato riportato 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 scadutoo revocato controllando le relative liste nel registro dei certificati o il relativo servizio di validazione.

4.6 Rinnovo del certificato

Per rinnovo del certificato si intende il rilascio di un nuovo certificato al Richiedente senza modificare la chiave pubblica o qualsiasi altra informazione sul certificato. Infocert non prevede il rinnovo del certificato mantenendo la stessa chiave pubblica.

4.6.1 Circostanze per il rinnovo del certificato

InfoCert manderà un'avviso di scadenza un mese prima della scadenza del certificato, ma non prevede il rinnovo, solo nuove emissioni.
In caso di certificati autenticazione Client, non e' prevista la spedizione di un avviso di scadenza.

4.7 Riemissione del certificato con rigenerazione delle chiavi

Consiste nella creazione di un nuovo certificato con una nuova chiave pubblica e numero di serie mantenendo le stesse informazioni del Soggetto

4.7.1 Circostanze per la riemissione del certificato

E' necessario generare delle nuove chiavi qualora si voglia richiedere la riemissione del certificato. Il nuovo certificato avrà i medesimi dati del subject DN mentre potrà avere valori differenti di periodo di validità, key identifiers, CRL ed OCSP distribution points ed essere firmato da una differente chiave di CA.

4.7.2 Richiesta di riemissione del certificato

La richiesta di riemissione del certificato è validata dalla CA secondo quanto specificato al par. 3.2.5 e 4.1.

4.7.3 Elaborazione delle richieste di riemissione del certificato

L'elaborazione rispetta quanto specificato al par. 4.2.

4.7.4 Notifica al titolare della riemissione del certificato

Vedi par. 4.3.2.

4.7.5 Accettazione del certificato riemesso

Vedi par. 4.4.1

4.7.6 Pubblicazione del certificato riemesso

No Stipulation

4.7.7 Notifica ad altri soggetti della riemissione del certificato

Vedi par. 4.4.3

4.8 Modifica del certificato

No Stipulation

4.9 Revoca e sospensione del certificato

La revoca di un certificato ne toglie la validità prima della scadenza prestabilita. I certificati revocati 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.

La verifica può essere fatta anche attraverso il servizio online OCSP.

La sospensione toglie la validità del certificato per un periodo temporaneo. Per i certificati emessi secondo il presente CPS, **non** è prevista la sospensione.

4.9.1 Motivi per la revoca

4.9.1.1 Circostanze per la revoca del certificato del richedente

Le condizioni per cui deve essere effettuata la richiesta di revoca entro 24 ore sono le seguenti:

- l'organizzazione informa la CA che la richiesta del certificato non era stata autorizzata, e non intende autorizzarla retroattivamente;
- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
  - sia venuta meno la segretezza della chiave;
  - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
- si scopre che l'uso di un FQDN o di un indirizzo IP contenuto nel certificato non è più consentito (per es. quando il titolare del dominio e/o della rete non ha rinnovato la registrazione, a seguito di un provvedimento dell'autorità giudiziaria, ecc);

Le condizioni per cui deve essere effettuata la richiesta di revoca entro 5 giorni sono le seguenti:

- il Soggetto non riesce più ad utilizzare la chiave in suo possesso (rottura del dispositivo in cui è memorizzata)
- si verifica un cambiamento dei dati del Soggetto presenti nel certificato, tale da rendere detti dati non più corretti e/o veritieri (per es. cessazione della società);
- termina il rapporto tra il Soggetto e la CA, ovvero tra il Richiedente e la CA;
- viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo;
- cessazione dell'attività della CA oppure perdita del suo diritto di emettere certificati conformi ai Requisiti [BR] (in mancanza di una CA sostitutiva che si faccia carico del servizio di revoca e pubblicazione delle informazioni sullo stato dei certificati);
- si scopre che il certificato contiene informazioni errate e/o fuorvianti;
- il certificato viene usato in modo improprio e/o illecito;
- si scopre che un certificato di tipo wildcard viene usato per autenticare un FQDN subordinato in modo fraudolento;

- errato profilo del certificato, a causa di un errore della CA (es. valori errati nelle estensioni);
- si scopre che il certificato non è conforme ai requisiti del CABForum sotto qualche aspetto.
- provvedimento dell'autorità giudiziaria;

4.9.1.2 Circostanze per la revoca del certificato della CA subordinata

No Stipulation

4.9.2 Chi può richiedere la revoca

La revoca può essere richiesta da

- Dal legale rappresentante (Richiedente) dell'organizzazione proprietaria del dominio (in caso di certificati di autenticazione siti WEB) o persona fisica dotata di procura, in qualsiasi momento e per un qualunque motivo.
- Terze Parti coinvolte (Es: Relying Parties Application Software Suppliers) possono segnalare alla CA ragionevoli ed importanti cause ai fini revoca del certificato. Inoltre, chiunque può segnalare alla CA fatti o circostanze che possono, secondo i casi, indurre la CA a reputare necessaria la revoca del certificato.
- Nel caso di certificato PSD2, le NCA che hanno rilasciato il numero di autorizzazione al prestatore di servizi di pagamento (PSP), presente nel certificato.
- L'Autorità giudiziaria

Il certificato può essere revocato d'ufficio dalla CA.

4.9.3 Procedure per richiedere la revoca

Il Richiedente può richiedere la revoca del certificato compilando l'apposito modulo messo a disposizione sul sito della CA, 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 e firmata digitalmente

La CA verifica l'autenticità della richiesta e procede alla revoca del certificato.

Nel caso di certificato PSD2 e la richiesta sia giunta da NCA, la CA investigherà sul motivo di tale richiesta.

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

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

4.9.4 Periodo di grazia della richiesta di revoca

Il periodo di grazia della richiesta di revoca è il tempo che può intercorrere tra l'identificazione di un evento a fronte del quale sia necessario richiedere la revoca del certificato e il momento di invio

della richiesta di revoca alla CA. Se la chiave privata corrispondente al certificato viene smarrita o compromessa il Richiedente deve richiedere la revoca del certificato quanto prima possibile.

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

La richiesta viene evasa entro 24 ore nei casi più gravi o 5 giorni negli altri casi. Non appena la richiesta viene autenticata correttamente, viene elaborata.

La richiesta di revoca che proviene da Terze Parti coinvolte che segnala alla CA ragionevoli ed importanti cause ai fini della revoca del certificato, viene presa in carico fornendo un rapporto preliminare al richiedente il certificato ed ai soggetti coinvolti nella richiesta entro 24 ore. Nel caso in cui si accerti la necessità di revocare il certificato, la CA in accordo col richiedente e le entità coinvolte, decide la data in cui il certificato verrà revocato. In ogni caso la data di revoca non deve superare i termini descritti precedentemente. La data deve essere concordata tenendo presente alcuni aspetti quali gli impatti della revoca, il tipo di problema rilevato, il numero di certificati coinvolti, la provenienza della richiesta (esempio autorità giudiziaria) e la legislazione vigente.

4.9.6 Verifica della revoca da parte degli utenti del certificato

Prima di fare affidamento sulle informazioni inserite nel certificato, l'utente deve confermare la validità del certificato secondo quanto previsto dagli standard IETF PKIX, comprendendo il controllo di validità, della concatenazione dei nomi emittente-soggetto, dei limiti nella policy e nell'utilizzo della chiave, dello stato di revoca tramite CRL o servizio OCSP per ogni certificato nella catena.

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) e rimane valida per 24 ore. 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 attestato utilizzando quale riferimento temporale la data fornita dal sistema di Time Stamping Authority InfoCert e una registrazione viene riportata nel giornale di controllo per attestare la pubblicazione in oggetto. 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 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

La pubblicazione della CRL viene effettuata dopo la sua generazione. Generalmente avviene in pochi minuti e non supera l'ora.

4.9.9 Servizi online di verifica dello stato di revoca del certificato

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

4.9.10 Requisiti per la verifica on-line

La CA supporta, per le richieste, il metodo GET come descritto in RFC 6960. In conformita' con CabForum, i risponditori OCSP non rispondono con lo stato 'good' per i certificati che non sono stati rilasciati

4.9.11 Altre forme per pubblicare le revoche

No Stipulation

4.9.12 Requisiti speciali in caso di compromissione chiave in caso di riemissione

No Stipulation

4.9.13 Motivi per la sospensione

No Stipulation

4.9.14 Chi può richiedere la sospensione

No Stipulation

4.9.15 Procedure per richiedere la sospensione

No Stipulation

4.9.16 Limiti al periodo di sospensione

No Stipulation

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 sono aggiornate entro 5 minuti, quelle della CRL ogni ora.

4.10.2 Disponibilità del servizio

Il servizio OCSP e le CRL sono disponibili 24 ore per 7 giorni la settimana. La risposta in entrambi casi viene fornita entro 3 secondi dalla ricezione della corrispondente richiesta.

4.10.3 Caratteristiche opzionali

No Stipulation

4.11 Disdetta dai servizi della CA

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

4.12 Deposito presso terzi e recovery della chiave

No Stipulation

5 MISURE DI SICUREZZA E CONTROLLI

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

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

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

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 situati 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 a 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.

5.2.2 Numero di persone richieste per lo svolgimento delle attività

La gestione delle chiavi private della CA avviene in ambiente protetto e con la partecipazione di due soggetti designati ('dual control').
Per l'emissione dei certificati OV, EV e QWAC sono necessari almeno due 'Validation Specialist'.

5.2.3 Identificazione e autenticazione per ciascun ruolo

A tutto il personale è richiesto di autenticarsi nei sistemi CA, e RA prima di poter accedere ai sistemi necessari per poter svolgere i propri ruoli.

5.2.4 Ruoli che richiedono la separazione dei compiti

Il personale che ricopre ruoli riguardanti il servizio di CA non puo' ricoprire uno dei ruoli chiave definiti al § 5.2.1.

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 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.

In particolare il personale ' Validation Specialist' viene formato su PKI, procedure di riconoscimento e validazione, minacce, requisiti del CabForum ([BR] e [EVGL]). A richiesta viene fornita la documentazione di tale formazione.

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

No Stipulation.

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

Il personale non dipendente che partecipa all'emissione dei certificati è sottoposto alle medesime condizioni funzionali e di sicurezza del personale dipendente che opera nelle medesime posizioni.

5.3.8 Documentazione fornita al personale

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.
Per ogni ruolo viene fornita la documentazione o gli estremi necessari allo svolgimento dei compiti. In particolare il presente CPS, i Baseline Requirements, le EV Guidelines del CabForum

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 ai sistemi PKI.
Vengono conservati tutti i dati e i 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, le registrazioni del certificato, la generazione, la diffusione, ed eventualmente la revoca/sospensione.
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 ed e' reso disponibile, previa richiesta, agli Auditors.

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita dal 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

No Stipulation

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 delle registrazioni

5.5.1 Tipi di registrazioni archiviati

Vengono redatti e archiviati le registrazioni relative ai più importanti eventi di una Certification Authority.

5.5.2 Periodo di conservazione degli archivi

Le registrazioni vengono conservate per 20 anni datta Certification Authority nel Sistema di Conservazione dei documenti Infocert.

5.5.3 Protezione delle registrazioni

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

5.5.4 Procedure di backup delle registrazioni

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

5.5.5 Requisiti per la marcatura temporale delle registrazioni

No Stipulation

5.5.6 Sistema di memorizzazione degli archivi

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

5.5.7 Procedure per ottenere e verificare le informazioni contenute negli archivi

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema di conservazione e dell'intera infrastruttura tecnica della CA. Il sistema di conservazione prevede il recupero, la verifica di integrità delle informazioni archiviate.

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.

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. Di seguito le attività principali:

- Apertura di un incidente di sicurezza
- Escalation come previsto dalla gestione incidenti con comunicazione immediata agli stakeholder

- Comunicazione immediata a CamerFirma (root della subCA InfoCert)
- Spegnimento del servizio con chiave compromessa
- Cancellazione chiave privata dall'HSM
- Comunicazione ad AGID (Supervisory Body) per la tempestiva rimozione della chiave dalla TSL
- Comunicazione all'Organismo di certificazione CAB
- Comunicazione ai clienti, siano essi soggetti del certificato o richiedenti, e agli utenti tramite comunicazione diretta, ove disponibile, e tramite comunicazione sul sito InfoCert
- Valuterà CamerFirma in base al tipo di compromissione se revocare il certificato di root e tutti i certificati emessi o solo quelli dopo una certa data.

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

Nel caso di cessazione dell'attività di certificazione, InfoCert comunicherà questa intenzione all'Autorità di vigilanza (AgID) all'ente certificatore (CAB) con un anticipo di almeno 6 mesi indicando, eventualmente, il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione ed evidenze. Con pari anticipo InfoCert informa della cessazione delle attività tutti i possessori di certificati emessi dalle proprie CA e gli Utenti mediante pubblicazione sulla pagina principale del sito di una nota informativa. 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.

Maggiori dettagli sono presenti nel documento TSP Termination CA v. 1.3 del 08/07/2019 [TP] disponibile presso il certificatore.

6 CONTROLLI TECNICI DI SICUREZZA

6.1 Installazione e generazione della coppia di chiavi

6.1.1 Generazione della coppia di chiavi

6.1.1.1 Generazione della coppia di chiavi della CA

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

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

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

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

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

6.1.1.2 Generazione della coppia di chiavi della RA

No Stipulation

6.1.1.3 Generazione coppia di chiavi del Richiedente

Ogni richiesta di chiave pubblica che non soddisfa i requisiti presenti nei §6.1.5 e §6.1.6 o se si tratta di chiave notoriamente debole, verra' rifiutata.
La CA Infocert genera la coppia di chiavi solo per i certificati di autenticazione di tipo Client su richiesta del Richiedente.

6.1.2 Consegna della chiave privata al Richiedente

La CA fornisce la coppia di chiavi al Richiedente, per i soli certificati di autenticazione Client, e tutta la catena di certificazione, mediante PKCS#12 protetto da Password.
La CA revochera' tutti i certificati corrispondenti alla chiave privata, nel caso in cui venisse comunicata ad un Richiedente non autorizzato.

6.1.3 Consegna della chiave pubblica alla CA

Il richiedente genera la chiave privata e sottomette la chiave pubblica alla CA attraverso la CSR durante il processo di richiesta descritto sopra. La richiesta è firmata.

6.1.4 Consegna della chiave pubblica della CA 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. Il certificato viene reso pubblico mediante l'inclusione negli elenchi delle Root CA affidabili gestiti dai principali produttori di sistemi operativi e browser e mediante la Trust-service Status List (TSL) pubblicata sul sito dell'Agid.

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

6.1.6 Controlli di qualità e generazione della chiave pubblica

La CA conferma che le chiavi pubbliche soddisfano i requisiti presenti al §6.1.6 del [BR]

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 l'autenticazione dei client e dei siti web.

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/o 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.

6.2.2 Controllo multi-utente 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

No Stipulation

6.2.4 Backup della chiave privata di CA

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

6.2.5 Archiviazione della chiave privata di CA

No Stipulation

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

No Stipulation

6.2.7 Memorizzazione della chiave privata su modulo crittografico

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

6.2.8 Metodo di attivazione della chiave privata

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

6.2.9 Metodo di disattivazione della chiave privata

No Stipulation

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

Vedere par. 6.2.1

6.3 Altri aspetti della gestione delle chiavi

6.3.1 Archiviazione della chiave pubblica

Vedere paragrafo 5.5

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.

Attualmente il certificato della CA ha una durata di 16 anni, i certificati emessi a persona fisica o giuridica hanno validità non superiore ai 2 anni.

6.4 Dati di attivazione della chiave privata

6.4.1 Generazione dei dati di attivazione e installazione

La generazione dei dati di attivazione avviene in accordo alle specifiche dei produttori degli HSM e secondo le pratiche di sicurezza adottate dal certificatore.

6.4.2 Protezione dei dati di attivazione

La protezione dei dati di attivazione dei certificati e' a carico dei Richiedenti. Per le chiavi di CA si veda par. 6.1.1

6.4.3 Altri aspetti relativi ai dati di attivazione

No Stipulation

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 (tramite procedure di 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.

6.5.2 Rating di sicurezza degli elaboratori

No stipulation

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 Riferimento temporale

Infocert fornisce un servizio di validazione temporale qualificato. Per la marcatura temporale fare riferimento al Manuale Operativo ICERT-INDI-TSA presente sul sito del prestatore di servizi fiduciari InfoCert.
I sistemi di elaborazione vengono mantenuti sincronizzati attraverso il medesimo riferimento temporale utilizzato per la marcatura temporale.

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; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.
InfoCert utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.
In Appendice il tracciato dei certificati della root e delle subCA.

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 419 312-5.
Per le estensioni vedere Appendice.

7.1.2.1 Certificati della Root CA

Vedi Appendice A

7.1.2.2 Certificati di CA subordinata

Vedi Appendice A

7.1.2.3 Certificati dei Richiedenti

Vedi §7.1.2.5

7.1.2.4 Tutti i certificati

Ulteriori estensioni e/o valori aggiuntivi nelle estensioni possono essere aggiunte purche' conformi a §7.1.2.5

7.1.2.5 Applicazione RFC 5280

I certificati emessi dalla CA Infocert rispettano sia la specifica RFC 5280 che i Requisiti e le linee del CabForum; [BR] e [EVG]

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.

7.1.4.1 Informazioni sull'emittente

Il contenuto del campo Issue DN corrisponde al DN della CA emittente

7.1.4.2 Informazioni sul titolare

Vedi §3.2.2 e § 3.2.3

7.1.4.2.1 Estensione SAN

Vedi §7.1.2.5

7.1.4.2.2 Campi del Subject Distinguished Name

Vedi §7.1.2.5

7.1.4.3 Informazioni sui certificati di Root CA e SubCA

7.1.4.3.1 Campi del Subject Distinguished Name

Vedi §7.1.2.5

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.

7.1.7 Uso dell'estensione PolicyConstraints

No Stipulation

7.1.8 Sintassi e semantica delle policy

Vedi §7.1

7.1.9 Regole di elaborazionedelle'stensione CertificatePolicies

No Stipulation

7.2 Formato della CRL

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

7.2.1 Numero di versione

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

7.2.2 Estensioni della CRL

Per le estensioni della CRL si veda l’appendice B

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 l’appendice B.

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 rilasciata ogni anno. In questo periodo vengono eseguite due o più sessioni di controllo.
La valutazione di conformità è pubblicata sul sito entro tre mesi dal suo rilascio.

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, 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.

8.6 Comunicazione dei risultati delle verifiche

Il Rapporto di Audit prodotto dal CAB viene inviato all'Agenzia per l'Italia Digitale (AgID), e a "AC Camerfirma S.A" che, essendo la CA Root che certifica la sub-CA di InfoCert, tiene i rapporti con Mozilla e comunica a quest'ultima i risultati dell'audit.

La valutazione di conformità viene condivisa con i responsabili del servizio e viene pubblicata entro e non oltre tre mesi dalla data dell'audit.

Gli audit interni vengono svolti in aderenza ad un programma di audit annuale e prendono in considerazione aspetti specifici del servizio, nonché aspetti più ampi relativi all'ambito della Certification Authority. I risultati di questi audit sono comunicati al responsabile del servizio e a tutte le persone direttamente coinvolte.

8.7 Self Audits

Durante il periodo in cui la CA emette certificati, l'auditor interno si occupa delle ispezioni di audit periodiche o aperiodiche. L'auditor interno controlla la qualità del servizio coordinando o eseguendo audit periodici con cadenza trimestrale, sull'emissione di certificati SSL: verifica a campione dei certificati emessi (3%), il loro ciclo di vita e le evidenze in essere, relative ai controlli effettuati ai fini del rilascio dei certificati stessi. L'auditor interno ha anche il compito di verificare che il servizio di rilascio dei certificati sia conforme a quanto descritto nel CP/CPS, negli standard ETSI e nelle linee guida di CABForum.

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

9.1.1 Tariffe per il rilascio e il rinnovo dei certificati

Le tariffe sono disponibili presso 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.

9.1.2 Tariffe per l'accesso ai certificati

No Stipulation

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

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:

- 10.000.000 euro per singolo sinistro;
- 10.000.000 euro per annualità.

9.2.2 Altre attività

No Stipulation

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

No Stipulation

9.3.3 Responsabilità di protezione delle informazioni confidenziali

No Stipulation

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 [DLGS196] e nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018 [GDPR].

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, date di revoca e di sospensione del certificato, non sono considerati dati personali.

9.4.4 Titolare del trattamento dei dati personali

InfoCert S.p.A.
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.
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

No Stipulation

9.5 Proprietà intellettuale

9.6 Dichiarazioni e garanzie

9.6.1 Dichiarazioni e garanzie della CA

InfoCert mantiene la responsabilità per l'osservanza delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto, ai sensi dell'art. 2.4.1. dell'Allegato al Regolamento di esecuzione UE 2015/1502 della Commissione.

9.6.2 Dichiarazioni e garanzie della RA

In quest'ultimo caso, la rappresentanza si esplica tramite mandato conferito da InfoCert all'Ufficio di Registrazione (di seguito anche "Registration Authority" o RA), nel quale vengono definiti il regime di responsabilità e gli obblighi delle parti. In particolare, l'Ufficio di Registrazione si impegna a svolgere l'attività di registrazione nel rispetto della normativa vigente e delle procedure di cui ai

Manuali Operativi, con particolare riferimento all'identificazione personale certa di coloro che sottoscrivono la richiesta di certificazione digitale ed a trasmettere i risultati di tali attività ad InfoCert.

9.6.3 Dichiarazioni e garanzie dei Richiedenti

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

9.6.4 Dichiarazioni e garanzie degli utenti

Vedi §4.5.2

9.6.5 Dichiarazioni e garanzie di altri partecipanti

No Stipulation

9.7 Limitazione di garanzia

il Certificatore non presta alcuna garanzia (i) sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal Richiedente; (ii) su usi della chiave privata, del dispositivo sicuro di firma – quando presente - e/o del certificato, che siano diversi rispetto a quelli previsti dalle norme vigenti e dal presente Manuale Operativo; (iii) sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali; (iv) sulla validità e rilevanza, anche probatoria, del certificato - o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito (v) sulla segretezza e/o integrità di qualsiasi messaggio, atto o documento associato al certificato o confezionato tramite le chiavi a cui il certificato è riferito.
Il Certificatore garantisce unicamente il funzionamento del Servizio, secondo i livelli indicati al paragrafo 9.17 del Manuale Operativo.

9.8 Limitazione di responsabilità

Il Certificatore non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti e/o, eventualmente, degli *hash* trasmessi dalla procedura informatica indicata dal Richiedente, non assumendo alcuna responsabilità.
Fatto salvo il caso di dolo o colpa, il Certificatore non assume responsabilità per danni diretti e indiretti subiti da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificato rilasciati in base alle previsioni del presente Manuale e delle Condizioni Generali dei Servizi di Certificazione.

InfoCert non è responsabile di qualsiasi danno diretto e/o indiretto derivante in via anche alternativa (i) dalla perdita, (ii) dalla impropria conservazione, (iii) da un improprio utilizzo, degli strumenti di identificazione e di autenticazione e/o (iv) dalla mancata osservanza di quanto sopra, da parte del Richidente.
Il Certificatore, inoltre, fin dalla fase di formazione del Contratto per i servizi di Certificazione (di seguito, anche "Contratto"), e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e della rete internet.
InfoCert, salvo il caso di dolo o colpa, non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Richiedente e/o a terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati da parte di terzi non autorizzati da InfoCert.

9.9 Indennizzi

9.9.1 Indennizzi da parte della CA

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

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

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo improprio del servizio di certificazione o al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili ad InfoCert, quali, a titolo esemplificativo, scioperi, sommosse, terremoti, atti di terrorismo, tumulti popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari hardware e/o dei software utilizzati dal Richiedente

9.9.2 Indennizzi da parte dei Richiedenti

No Stipulation

9.9.3 Indennizzi da parte degli utenti

No Stipulation
.

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. Il Contratto di certificazione tra il Certificatore e il Soggetto ha durata pari a quella del certificato emesso indicata nel campo "validità (validity)" dello stesso.

9.10.2 Risoluzione

Il Contratto si risolverà di diritto con contestuale interruzione del Servizio e revoca del certificato emesso, nel caso in cui il Titolare e/o il Richiedente sia inadempiente rispetto alle previsioni contenute nelle clausole del Contratto di cui all'art. 3 (Responsabilità del Titolare e del Richiedente); art. 4.6 (Proprietà Intellettuale), art. 8 (Obblighi del Titolare); art. 11 (Corrispettivi), art. 12.3 (sull'obbligo di notifica dei casi e motivi di sospensione e revoca del certificato); se applicabile, art. 45 (Ulteriori Obblighi del Titolare e del Richiedente), se applicabile, art. 47 (Ulteriori obblighi del Titolare) nonché a quanto previsto dal presente Manuale Operativo. La risoluzione si verificherà di diritto quando la parte interessata dichiari all'altra a mezzo PEC o lettera raccomandata a.r., che intende avvalersi della presente clausola.
Nel caso in cui il Richiedente sia un consumatore, le controversie civili inerenti il Contratto concluso dal consumatore sono devolute alla competenza territoriale inderogabile del giudice del luogo di residenza o di domicilio di questo.
Il consumatore può servirsi, su base volontaria, dei metodi di risoluzione extragiudiziale delle controversie previsti dal Codice del Consumo italiano e dalle altre norme di legge applicabili in materia.
Si informa altresì che, ai sensi e per gli effetti del Regolamento UE n. 524/2013, per la risoluzione delle controversie relative ai contratti online e ai servizi offerti online, vi è la possibilità di ricorrere al procedimento di Online Dispute Resolution (ODR), previsto dalla Commissione Europea e raggiungibile al seguente *link*: https://webgate.ec.europa.eu/odr/ .
Il Certificatore ha diritto di recedere in qualsiasi momento dal Contratto per i Servizi di Certificazione, con un preavviso di 30 giorni e, conseguentemente, di revocare il certificato.
In tutti i casi in cui il Richiedente sia inadempiente rispetto alle obbligazioni assunte, il Certificatore potrà sospendere l'erogazione del Servizio, anche attraverso la sospensione del Certificato. In particolare, in caso di mancato pagamento del corrispettivo del Servizio, InfoCert avrà comunque diritto di sciogliere il Contratto con il Richiedente in ogni momento, senza alcun preavviso e onere, e conseguentemente revocare ogni certificato emesso.
In caso di recesso da parte del Richiedente o revoca del certificato, il corrispettivo è comunque dovuto e se già versato è interamente trattenuto da InfoCert anche a titolo di corrispettivo per il recesso.
In tutti i casi di risoluzione, cessazione dell'efficacia del Contratto e suo scioglimento, saranno salvi gli effetti prodotti dal Contratto fino a tale momento.
Il Richiedente prende atto che, in caso cessazione del Contratto, per qualsiasi causa essa avvenga, non sarà più possibile usufruire del Servizio.

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata revoca del certificato.

9.11 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel §1.5.2.

9.12 Revisione del Manuale Operativo

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

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.

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:	11/02/2020
Descrizione modifiche:	Aggiunto riferimenti alla nuova SubCa $ 1.1 aggiornamento versioni BR ed EV guidelines CabForum § 1.3.4 aggiunto utilizzo termine titolare § 1.3.5 aggiunto utilizzo termine Relying Party § 1.5.1 aggiunto paragrafo § 1.6.3 aggiunto paragrafo § 2.1 aggiunto url nuove pagine di test per la nuova subCa § 3.2.6 aggiunto paragrafo § 3.3 modificato titolo. Aggiunto paragrafi 3.3.1 e 3.3.2. § 3.4 aggiunto paragrafo § 4.4.3 aggiunto notifica ai CT Log § 4.6 miglioramento descrizione § 4.7 miglioramento descrizione. Aggiunto paragrafi 4.7.4, 4.7.5, 4.7.6, 4.7.7 § 4.7.1 modificato titolo § 4.9 miglioramento descrizione, aggiunti par. 4.9.1.2 § 4.9.8 miglioramento descrizione § 5.2.2 aggiunto paragrafo § 5.2.3 aggiunto paragrafo § 5.2.4 aggiunto paragrafo § 5.3.3 miglioramento descrizione § 5.3.5 inserito No Stipulation § 5.3.7 aggiunta condizioni § 5.3.8 modificato titolo e migliorata descrizione

	§ 5.3.8 miglioramento descrizione § 5.5.2 modificato titolo § 5.5.3 miglioramento descrizione § 5.7.3 migliorata descrizione § 5.8 Migliorata descrizione § 6.1.1.1 modificato titolo § 6.1.1.2 aggiunto paragrafo § 6.1.1.3 aggiunto paragrafo § 6.1.2 migliorata descrizione § 6.1.4 migliorata descrizione § 6.1.6 migliorata descrizione § 6.3.2 modificata durata certificati autenticazione Client e Server § 6.4.1 aggiunto paragrafo § 6.4.2 aggiunto paragrafo § 6.4.3 aggiunto paragrafo § 6.5.2 aggiunto paragrafo § 7.1.2 aggiunti paragrafi 7.1.2.1, 7.1.2.2, 7.1.2.3, 7.1.2.4, 7.1.2.5 § 7.1.4 aggiunti paragrafi 7.1.4.1, 7.1.4.2, 7.1.4.2.1, 7.1.4.2.1, 7.1.4.2.2, 7.1.4.3, 7.1.4.3.1 § 7.1.7 aggiunto paragarafo § 7.1.8 aggiunto paragrafo § 7.1.9 aggiunto paragrafo § 6.8 aggiunto paragrafo § 8.6 aggiunto paragrafo § 8.7 aggiunto paragrafo § 9.6 modificato titolo § 9.6.1 modificato titolo § 9.6.2 aggiunto paragrafo § 9.6.3 aggiunto paragrafo § 9.6.4 aggiunto paragrafo § 9.6.5 aggiunto paragrafo § 9.9.1 aggiunto paragrafo § 9.9.2 aggiunto paragrafo § 9.9.3 aggiunto paragrafo § 9.12.2 migliorata descrizione § 9.12.3 migliorata descrizione § 9.16.4 aggiunto paragrafo § 9.16.5 aggiunto paragrafo
Motivazioni:	Nuova root SubCa Allineamento indice a RFC3647 Sostituzione verifica n/a con No Stipulation Aggiornamento versioni BR ed EV guidelines CabForum

Versione/Release n°:	**3.1**
Data Versione/Release:	27/11/2019
Descrizione modifiche:	Aggiunto riferimenti ai certificati di autenticazione Client $ 1.1 aggiornamento versioni BR ed EV guidelines CabForum $ 1.2 correzione OID $ 3.2.5 telefonata come modalità ulteriore di validazione dominio
Motivazioni:	Revisione annuale Emissione certificati autenticazione Client Aggiornamento versioni BR ed EV guidelines CabForum

Versione/Release n°:	3.0
Data Versione/Release:	30/11/2018
Descrizione modifiche:	$ 1.1 Aggiornamento versione documenti CABForum, descrizione PSD2, corretto errore policy CABForum $ 1.2 Aggiornamento OID e descrizione $ 3.1.5 CommonName deprecato $ 3.2.5 Istruttoria da parte della CA per certificati PSD2 $ 3.2.5 Aggiornate modalità di validazione del dominio $ 4.2 Elaborazione richiesta PSD2 $ 4.9 Revoca, revisione paragrafo
Motivazioni:	Revisione annuale Emissione certificati conformi PSD2 Revisione controlli Modifica ragione sociale TecnoInvestimenti

Versione/Release n°:	2.1
Data Versione/Release:	20/06/2018
Descrizione modifiche:	$ 1.5.1 Aggiornamento riferimenti $ 9.2.1 Copertura assicurativa $ 9.9 Indennizzi
Motivazioni:	Aggiornamento numero call center Aggiornamento massimali assicurazione

Versione/Release n°:	2.0
Data Versione/Release:	06/12/2017
Descrizione modifiche:	Definizioni: aggiornate alcune definizioni Correzioni ortografiche e di forma Eliminati riferimenti al Domain Validation Descritte le limitazioni delle attività previste per RA Aggiunte motivi di revoca Riportati i link delle CA e subCA afferenti al presente manuale. Corretta la numerazione del capitolo 4 in conformità a RFC 3647 Revisione capitolo 9
Motivazioni:	Allineamento del manuale ai requirements di CAB Forum più recenti: Baseline Req 1.5.1 e Extended Validation 1.6.6

Versione/Release n°:	1.1
Data Versione/Release:	08/02/2017
Descrizione modifiche:	Definizioni: aggiornate alcune definizioni Introduzione: migliorata la descrizione del servizio OID per certificato non qualificato 1.3.76.36.1.1.19.2 $ 4.2.1 Aggiunti dettagli sulla CSR

	$ 4.2.4 Rivisti gli SLA Correzione forma e ortografia
Motivazioni:	Allineamento del manuale ai requirements di CAB Forum più recenti del 7 gennaio 2017

Versione/Release n°:	**1.0**
Data Versione/Release:	12/12/2016
Descrizione modifiche:	
Motivazioni:	nuova emissione del documento

9.12.1 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.

9.12.2 Periodo e meccanismo di notifica

Il Manuale operativo viene riesaminato ad aggiornato almeno una volta ogni anno. Anche se non vengono apportate modifiche al documento, il numero di versione viene aumentato, viene aggiunta una voce di log e viene aggiornata la data di riesame.

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web di InfoCert (indirizzo: http://www.firma.infocert.it/doc/manuali.htm);
- in formato cartaceo può essere richiesto alle Registration Authority o al contatto per gli utenti finali.

9.12.3 Casi nei quali l'OID deve cambiare

La revisione del CPS non prevede modifiche agli OID.

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] *non utilizzato*

[4] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018)

[5] *non utilizzato*.

[6] *non utilizzato*

[7] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori e relative normative nazionali di recepimento

[8] Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio, del 25 novembre 2015 conosciuta come Payment Services Directive – PSD2.

[9] Regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza[1], 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.

9.16.1 Condizioni generali di servizio

Sono pubblicate sul sito web del certificatore.

9.16.2 Deleghe

La delega della validazione ad una RA è accompagnata da un'apposita convenzione tra InfoCert e l'organizzazione nominata Registration Authoority per InfoCert.

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

9.16.3 Invalidità

Se un tribunale dichiara non valida una disposizione del presente manuale operativo, le altre disposizioni rimangono valide. La CA modificherà le proprie procedure il minimo per rimanere più aderenti possibili alle linee guida.

9.16.4 Applicazione

Si rimanda alla contrattualistica che regolamenta il servizio

9.16.5 Forza maggiore

Si rimanda alla contrattualistica che regolamenta il servizio

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 (disponibilità minima mensile 99%)
Revoca e sospensione dei certificati.	Dalle 0:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione.	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi
Richiesta e/o verifica di marca temporale.	24hx7gg (disponibilità minima 99%)

Appendice A Certificati di root CA e gerarchia delle subCA

InfoCert Root CA 3
http://cert.infocert.it/ca3/root/CA.crt
numero di serie seriale: c35de37e34e4917f4a8d9f7c92bcaa4f9ee6afa
identificativo della chiave: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert Organization Validation SHA256 - CA 3
Autorità di certificazione:

- CN: InfoCert Root CA 3
- OU: WSA Trust Service Provider.
- O: InfoCert S.p.A..
- C:IT
- Numero di serie certificato: 44841e74619f52cb

http://cert.infocert.it/ca3/ovca/CA.crt
numero di serie: 7d04f008647c18b07ee55a1f5a45874c7b45855b

identificativo della chiave: 070bf5de8672fc47ade69234e42f8ae6a1a7b95a
identificativo della chiave dell'autorità: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert Extended Validation SHA256 - CA 3
Autorità di certificazione

- CN: InfoCert Root CA 3
- OU: WSA Trust Service Provider.
- O: InfoCert S.p.A..
- C:IT

http://cert.infocert.it/ca3/evca/CA.crt
numero di serie: 6b445ba522e87824cff71ce8444f9bb887f5e4b1
identificativo della chiave: 2495f85228f235c5b1856b458850c84719b3ef81
identificativo della chiave dell'autorità: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert CA3 OV CamerFirma trusted
Autorità di certificazione:

- CN:Global Chambersign Root – 2008
- O:AC Camerfirma S.A.
- SN:A82743287
- L:Madrid (see current address at www.camerfirma.com/address)
- C:EU
- Numero di serie certificato: 44841e74619f52cb

http://cert.infocert.it/ca3/ovcf/CA.crt
Numero di serie: 0249528bfbff7ddf
identificativo della chiave: 5f0ebbb9cf47920c26345605bfdc9d9e18bdc925
identificativo della chiave dell'autorità: 5b1bee037ba2dbe746c0c254aba150295ff156d7

InfoCert 2019 CA3 OV CamerFirma trusted
Autorità di certificazione:

- CN:Global Chambersign Root – 2008
- O:AC Camerfirma S.A.
- SN:A82743287
- L:Madrid (see current address at www.camerfirma.com/address)
- C:EU
- Numero di serie certificato: 00c9cdd3e9d57d23ce

http://cert.infocert.it/ca3/ovcf2019/CA.crt
Numero di serie: 31b31444fdd6c2a78f0a9c
identificativo della chiave: 8832bf09fb4239f472432068b8cfac8a92785d0c
identificativo della chiave dell'autorità: 5b1bee037ba2dbe746c0c254aba150295ff156d7

Appendice B Formato delle CRL e OCSP

Estensione	Valore

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

Valori ed estensioni per CRL e OCSP

Le CRL hanno le seguenti estensioni

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

La richiesta OCSP contiene i seguenti campi:

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

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	Stato della risposta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificato firmatario della risposta OCSP
Produced at	Data in formato GeneralizedTime che indica quando è stata generate la risposta OCSP
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash del DN dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente.
Serial Number	Numero di serie del certificato
thisUpdate	Data di verifica dello stato del certificato in formato GeneralizedTime

nextUpdate	Data in cui lo stato del certificato potrebbe essere aggiornato
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

OCSP Extensions

La richiesta OCSP può contenere le seguenti estensioni:

Extension	Value
nonce	Un numero arbitrario che può essere usato una sola volta. Crittograficamente lega una richiesta alla sua risposta per prevenire attacchi da replica. È contenuto in una requestExtensions nel caso della richiesta, mentre nel caso della risposta può essere contenuta in una responseExtensions.