Manuale Operativo

Firma Elettronica

Certificate Practice Statement

CODICE DOCUMENTO ICERT-INDI-FD

VERSIONE 3.2

DATA 18/07/2023

INFOCERT

TINEXTA GROUP

Questa pagina è lasciata
intenzionalmente bianca

1 Sommario

1.1 Introduzione al documento

1.1.1 Novità introdotte rispetto alla precedente emissione:

Versione/Release n° :	3.2	**Data Versione/Release**:	18/07/2023
Descrizione modifiche:	Nuovo logo InfoCert		
Motivazioni:	Rebranding		

Versione/Release n° :	3.1	**Data Versione/Release**:	28/09/2021
Descrizione modifiche:	Aggiornamento contatti		
Motivazioni:			

Versione/Release n° :	3.0	**Data Versione/Release**:	27/09/2019
Descrizione modifiche:	Revisione completa del manuale Aggiunto riferimenti CodeSign Aggiunto riferimenti Autenticazione Server e Porte Applicative		
Motivazioni:			

Versione/Release n° :	2.0	**Data Versione/Release**:	15/02/2016
Descrizione modifiche:	Revisione completa del manuale		
Motivazioni:			

Versione/Release n° :	1.0	**Data Versione/Release**:	11/07/2008
Descrizione modifiche:	Prima emissione		
Motivazioni:			

Il presente manuale ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCert per l’erogazione del servizio di certificazione della chiave pubblica di una coppia di chiavi asimmetriche, utilizzata per

- autenticazione in applicazioni operanti in ambito web (Client, Server Notrust, Porte applicative)
- firma e cifra della posta elettronica
- firma codice

Il Certificatore 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 annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

Il presente documento è denominato “Certificati Firma Elettronica -
Manuale Operativo” ed è caratterizzato dal codice documento: ICERT-INDI-FD.

Al documento sono associati gli Object Identifier (OID), descritti in seguito, che sono referenziati nell'estensione CertificatePolicy dei certificati, secondo l'utilizzo cui gli stessi sono destinati. Il significato degli OID è il seguente:

InfoCert certification-service-provider	1.3.76.36 1.3.76.36.1
certificate-policy	1.3.76.36.1.1
manuale-operativo-Servizio di Certificazione “Firma Elettronica”	1.3.76.36.1.1.8
manuale-operativo-Servizio di Certificazione “Firma Codice”	1.3.76.36.1.1.8.7
manuale-operativo-Servizio di Certificazione “Autenticazione Server NoTrust”	1.3.76.36.1.1.8.8

Il manuale è pubblicato in formato elettronico sul sito Web del Certificatore, all’indirizzo https://www.firma.InfoCert.it/documentazione/

1.2 Termini e definizioni

- **Certificatore:** è l’ente che fornisce il Servizio di Certificazione. Ai fini del presente documento Certificatore è InfoCert S.p.A.
- **Client:** è l’applicativo software, ad esempio un browser Web, utilizzato dall’utente che si connette ad un sito di un Web server certificato, con cui vuole instaura una comunicazione sicura e protetta.

- **Cliente o soggetto richiedente: e**nte, organizzazione o persona che richiede il servizio
- **Chiave Privata e Chiave Pubblica – cfr. [1]**
- **CSR:** Certificate Signing Request. Vedi PKCS#10
- **Dati per la creazione di una firma – cfr. [1]**
- **Dati per la verifica della firma – cfr. [1]**
- **Digest:** impronta del messaggio dopo l’applicazione dell’algoritmo crittografico SHA.
- **Nome Distintivo (Distinguished Name):** attributi del certificato che lo identificano.
- **Firma elettronica – cfr. [1]**
- **Firma elettronica qualificata – cfr. [1]**
- **Firma digitale *[digital signature]* – cfr. [1]**
- **PEM: a**cronimo di **P**rivacy **E**nhanced **M**ail, è uno standard per la trasmissione di posta sicura sulla rete Internet che si basa su tecniche crittografiche e firma digitale per la protezione dei dati trasmessi.
- **PKCS#10:** PKCS, acronimo di **P**ublic **K**ey **C**ryptography **S**tandards, è un insieme di standard per la crittografia a chiave pubblica sviluppati dai Laboratori RSA: definiscono la sintassi del certificato digitale e dei messaggi crittografati, in particolare il PKCS#10 definisce la struttura della richiesta per la certificazione della chiave pubblica di una coppia di chiavi asimmetriche.
- **PKCS#12: P**ublic **K**ey **C**ryptography **S**tandards numero 12. Il PKCS#12 è lo standard per la sintassi dello scambio di informazioni personali. Definisce la struttura di imbustamento capace di contenere sia la chiave privata sia il certificato ad essa relativo.
- **RSA:** Algoritmo di crittografia asimmetrica
- **Soggetto richiedente o Cliente:** Ente, organizzazione o persona che richiede il servizio
- **SHA256: l**a sigla SHA sta per Secure Hash Algorithm, è una funzione crittografica utilizzate per calcolare l’hash o digest. 256 sono il numero di bit del messaggio risultante
- **SSL: a**cronimo di **S**ecure **S**ockets **L**ayer, è il protocollo che consente di stabilire una comunicazione autenticata e riservata tra le parti comunicanti, client e server.
- **TSL:** Acronimo di **T**ransport **L**ayer **S**ecurity, è il protocollo che consente di stabilire una comunicazione autenticata e riservata tra le parti comunicanti, client e server. Successore del protocollo SSL.
- **Titolare:** il soggetto/entità, titolare del Certificato.
- **Utente:** chiunque verifichi il Certificato.
- **Web server:** è il software che consente di distribuire informazioni su Internet e riceve richieste da parte di un browser Web restituendo i dati richiesti.
- **X.509: s**tandard per la definizione della struttura del formato dei certificati digitali di chiave pubblica. Definisce, inoltre, le caratteristiche di un’Infrastruttura a Chiave Pubblica (PKI).

1.3 Riferimenti

Riferimenti tecnici

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come CAD)

1.3.1 Riferimenti tecnici

2. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile”

3. RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”
4. Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (2012) | ISO/IEC 9594-8:2014

1.4 Responsabile del Manuale Operativo

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

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telefono: 06 836691
Fax: 06 23328861
Call Center: consultare il link https://help.infocert.it/contatti/
Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

2 Caratteristiche del servizio

2.1 Soggetto fornitore

Il servizio di certificazione Firma Elettronica (nel seguito abbreviato in FD) viene fornito dall’Ente di Certificazione InfoCert S.p.A. secondo le procedure e le condizioni stabilite nel presente Manuale Operativo.

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

Tabella 2

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. di telefono	06 836691
N. Iscrizione Registro Imprese	Codice Fiscale 07945211006

N. partita IVA	07945211006
Sito web	https://www.infocert.it

2.2 Descrizione del servizio

Il servizio descritto riguarda la certificazione della chiave pubblica appartenente alla coppia di chiavi asimmetriche (chiave privata e chiave pubblica) del certificato, il cui utilizzo è:

- autenticazione a server web,
- autenticazione ad altra applicazione,
- firma e cifratura di posta elettronica,
- autenticazione codice
- autenticazione server no trust.
- autenticazione porte applicative

2.3 Soggetti destinatari del servizio

Il servizio di certificazione può essere richiesto da qualunque Ente o Organizzazione o Persona (denominato Cliente) che abbia sottoscritto un contratto con InfoCert per la fornitura di questo servizio.
InfoCert effettuerà al riguardo le opportune verifiche in fase di richiesta del servizio e potrà negare l’emissione del certificato in caso di falsità, incongruenze e difformità delle informazioni fornite.

2.4 Responsabile del servizio

Responsabile del servizio fornito è l’Ente Certificatore InfoCert. I riferimenti della persona da contattare per questioni riguardanti il servizio sono riportati al paragrafo 1.4.

3 Descrizione dei certificati

3.1 Formato del certificato e sua validità

I certificati emessi dall’Ente Certificatore è conforme al formato standard X.509 v3 [4].

La durata dei certificati è stabilita contrattualmente tra InfoCert e il Cliente: può essere una durata compresa tra 1 a 5 anni.

Gli obblighi e i diritti dell’Ente Certificatore e dei soggetti titolari che scaturiscono dal presente Manuale Operativo si intendono riferiti al periodo di validità del certificato emesso.

4 Procedure operative

La procedura per la certificazione di un titolare si compone delle seguenti fasi:

1. Richiesta ad InfoCert da parte del cliente di emissione del/i certificato/i
2. Controllo e validazione dei dati della richiesta da parte di InfoCert
3. Registrazione dei dati da parte di InfoCert
4. Emissione del certificato
5. Consegna al richiedente

4.1 Richiesta di emissione

4.1.1 Modalità di invio della richiesta

La richiesta di certificazione, a seconda della tipologia dei certificati richiesti e del relativo numero, deve essere inoltrata alla CA attraverso i vari canali messi a disposizione dall’ente certificatore.

I principali sono:

- casella di e-mail certificati.P12@InfoCert.it
- casella di e-mail dedicata al cliente/tipologia certificati
- applicativo web based con credenziali rilasciate al richiedente
- richieste applicative basate su integrazione di specifici servizi
- emissioni speciali seguite attraverso operatore dedicato

La richiesta deve essere autenticata tramite firma elettronica avanzata, che viene rilasciata ai soggetti che il Cliente avrà indicato come propri referenti.
Sono previste altre forme di autenticazione concordate col cliente a seconda dei certificati richiesti, del relativo numero e dal canale utilizzato.

La coppia di chiavi può anche essere generata presso il cliente che deve inviare una CSR (Certificate Signing Request) nel formato precedentemente concordato con il certificatore.

Nel caso di richieste multiple, il certificatore fornisce i tracciati da utilizzare, indicando i campi obbligatori rispetto alla tipologia di richiesta trattata. Una volta compilati secondo il tracciato suddetto, i file devono essere firmati tramite firma elettronica avanzata, che viene preventivamente rilasciata ai soggetti che il Cliente avrà indicato come propri referenti e inviati a InfoCert.

4.1.2 Caratteristiche della chiave pubblica da certificare

Per compatibilità con CAB-Forum l’algoritmo di digest deve essere almeno SHA256 e la lunghezza della chiave non deve essere inferiore ai 2048 bit.
L'algoritmo di crittografia asimmetrica da utilizzare è l'RSA.

La coppia di chiavi deve essere utilizzata in modo tale da prevenire l’eventuale compromissione, perdita, individuazione, modifica o utilizzo non autorizzato della chiave privata.

Nel caso in cui la coppia di chiavi venga generata dall’utente, l’operazione deve essere fatta in modo tale da prevenire l’eventuale compromissione, perdita, individuazione, modifica o utilizzo non autorizzato della chiave privata.

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

4.2 Controllo e validazione della richiesta

La richiesta viene controllata o dai servizi specifici applicativi o dall’ufficio incaricato InfoCert. Viene verificata la provenienza, l'integrità, le autorizzazioni del mittente e la sussistenza delle condizioni contrattuali. Se dovessero mancare informazioni necessarie per emettere il certificato, l’incaricato si metterà in contatto con il richiedente per chiarimenti.

InfoCert non darà corso all’emissione del certificato qualora i dati comunicati non risultino corretti o completi in base ai riscontri derivanti dalle verifiche

Durante il controllo, l’incaricato InfoCert, potrebbe richiamare il richiedente per verificare la veridicità delle informazioni.

4.3 Emissione del certificato

InfoCert, a fronte della consistenza della richiesta emette il/i certificato/i.

Il Cliente che ha sottoscritto il contratto ha facoltà di mettere a disposizione sul proprio sito il certificato di chiave pubblica corrispondente alla chiave privata con cui l’Ente Certificatore InfoCert sottoscrive i certificati di firma elettronica. Tale certificato è anche scaricabile dal sito del Certificatore alla voce “Prodotti e Servizi”, seguendo le procedure indicate nel sito medesimo. Il prelievo e il successivo inserimento di tale certificato nella lista dei certificati di CA “trusted” gestita dai client e server degli utenti consentiranno di validare correttamente l’intera catena di certificazione (certificato di applicazione e certificato di CA), permettendo così di verificare l’identità dell'applicazione comunicante.

4.4 Consegna al richiedente

Una volta emesso il certificato, il richiedente viene informato e riceve quanto richiesto attraverso la posta elettronica all’indirizzo fornito. Riceverà due messaggi separati.

Il primo messaggio, firmato dall’ente emettitore, contiene un file in formato zip con il file PKCS#12 generato e tutta la catena di certificazione per la corretta validazione dello stesso.

Il secondo messaggio contiene le password per l’utilizzo del file PKCS#12. In alternativa, se ha comunicato un numero di telefono la password viene inviata attraverso SMS.

Rimane a carico dell’utilizzatore finale provvedere alla corretta impostazione della propria postazione o dei propri servizi per l’utilizzo di tali certificati.

Nel caso in cui la richiesta venga effettuata mediante l’integrazione di servizi applicativi, il certificato o il PKCS#12 viene consegnato mediante lo stesso canale.

5 Ciclo di vita dei certificati

Il ciclo di vita di questo tipo di certificati in parte dipende sempre dall’utilizzo finale previsto e dagli accordi commerciali presi in fase di emissione. In questo capitolo vengono descritte le regola generali.

La revoca di un certificato rende **non validi** tutti gli utilizzi della corrispondente chiave privata effettuati successivamente al momento di revoca.

I certificati revocati sono inseriti in una lista di revoca (CRL) firmata dal Certificatore. La revoca di un certificato ha efficacia dal momento di pubblicazione della lista.

5.1 Revoca

Il Certificatore può eseguire la revoca del certificato su propria iniziativa, su richiesta del cliente o su richiesta del titolare. La revoca va richiesta nel caso si verifichino le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia venuta meno la segretezza della medesima, ovvero si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata stessa;
- il titolare non riesca più ad utilizzare il certificato in suo possesso;
- siano cambiati i dati presenti nel certificato;
- termini il rapporto tra il titolare e il Certificatore;
- sia stata appurata una condizione di non rispetto del presente Manuale Operativo;
- sia stato emesso un provvedimento dell’Autorità Giudiziaria.

5.1.1 Revoca su iniziativa del Certificatore

Il Certificatore attiva una richiesta di revoca con la seguente modalità:

1. il Certificatore comunica al cliente l’intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza;
2. la procedura di revoca del certificato viene completata con l’inserimento dello stesso nella lista dei certificati revocati o sospesi.

5.1.2 Revoca su iniziativa del Cliente

Il Cliente inoltra la richiesta di revoca tramite mail, firmata con firma elettronica avanzata di un referente autorizzato, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando indicare il “numero di serie” e il “nome distintivo” del certificato.

Il Certificatore, verificata l’autenticità della richiesta, procede alla revoca

5.1.3 Revoca su iniziativa del titolare

Il titolare inoltra la richiesta di revoca tramite mail, eventualmente firmata con firma elettronica avanzata di un referente autorizzato, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando indicare il “numero di serie” e il “nome distintivo” del certificato.

Il Certificatore, verificata l’autenticità della richiesta, procede alla revoca

5.2 Pubblicazione e frequenza di emissione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca (CRL), firmata dal Certificatore, immessa e pubblicata nel registro dei certificati (Directory LDAP) all’indirizzo indicato nell’estensione “CRL Distribution Point” presente nel certificato.
La CRL viene pubblicata in modo programmato ogni giorno.
L’acquisizione e consultazione della CRL è a cura degli utenti, ovvero Titolari. La CRL è emessa sempre integralmente. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l’ora di richiesta della revoca.

5.3 Validità e Rinnovo

Il certificato contiene al suo interno l’indicazione del periodo di validità nel campo "validità" (*validity*) con gli attributi "valido dal" (*not before*) e "valido fino al*“ (not after).*

5.4 NOTA

le date indicate negli attributi suddetti sono espresse nel formato

anno-mese-giorno-ore-minuti-secondi-timezone
{AAAAMMGGHHMMSSZ}

nella rappresentazione UTCTime prevista dallo standard di riferimento.

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

Per i certificati di firma elettronica il rinnovo consiste in una nuova emissione.Il Certificatore informerà il cliente via e-mail, con un preavviso di almeno 30 giorni, della imminente scadenza del certificato e della necessità di richiederne uno nuovo per garantire la continuità del servizio, con le modalità indicate nella comunicazione stessa. Altre modalita’ possono essere concordate con il cliente

La nuova richiesta sarà effettuata secondo le stesse modalità della prima.
Il Certificatore procederà alla generazione di un nuovo certificato nelle modalità previste per la prima emissione, ferma restando la verifica della sussistenza delle condizioni contrattuali.

La chiave privata di firma di cui sia scaduto il certificato della relativa chiave pubblica, non deve essere più utilizzata.

6 Tariffe e condizioni

Le tariffe per la prima emissione e per il rinnovo dei certificati sono stabilite dal contratto di servizio tra InfoCert e il Cliente.

Le revoche dei certificati sono gratuite.