MANUALE OPERATIVO

SSAS Policy
SSAS Practice Statement

CODICE DOCUMENTO	ICERT-INDI-SSAS
VERSIONE	1.0
DATA	16/03/2026

tinexta
infocert

SOMMARIO

INTRODUZIONE

1.1 Quadro generale — Servizio di firma qualificata remota

Il servizio di firma elettronica qualificata remota consente al Titolare di un certificato qualificato di generare firme o sigilli elettronici qualificati mediante l'utilizzo di un dispositivo per la creazione di firma qualificata (**QSCD**) in modalità remota, nel quale la chiave privata di firma è generata e custodita nello stesso QSCD in un ambiente sicuro da parte del QTSP che gestisce le chiavi per conto del Firmatario.

Nel modello di firma remota, la chiave privata associata al certificato qualificato non è detenuta direttamente dal Firmatario su un dispositivo fisico personale, ma è conservata e protetta all'interno di un sistema crittografico gestito da un prestatore di servizi fiduciari qualificato. Il servizio è progettato in modo da garantire che la chiave privata non sia esportabile e che il suo utilizzo avvenga esclusivamente secondo meccanismi di attivazione della firma che assicurano il controllo esclusivo del Firmatario.

In particolare, il sistema garantisce che:

- la coppia di chiavi di firma sia generata in ambiente sicuro all'interno del QSCD remoto;
- la chiave privata sia non esportabile e protetta contro accessi non autorizzati;
- l'utilizzo della chiave sia subordinato ad autenticazione del Firmatario e ad una sua richiesta esplicita di firma;
- siano adottate misure di tracciamento e controllo idonee a supportare verifiche di sicurezza e audit.

Il servizio è erogato in conformità al Regolamento [1] e successive modifiche, nonché agli standard tecnici applicabili, tra cui ETSI TS 119 431-1, che disciplina i requisiti di sicurezza, gestione e funzionamento dei sistemi di firma remota e dei meccanismi di attivazione della firma, nonché ETSI EN 319 401 e DS/EN 419241-1:2018.

Il presente Manuale Operativo descrive le politiche, le pratiche, le misure di sicurezza e i controlli adottati da Tinexta Infocert per garantire la corretta generazione, protezione e utilizzo delle chiavi di firma nel contesto del servizio di firma qualificata remota, nonché l'affidabilità del servizio e il rispetto del principio di controllo esclusivo del Firmatario.

La struttura del documento è allineata al framework IETF RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, utilizzato come guida.

1.2 Nome e identificativo del documento

Il presente documento è identificato dal codice documento **ICERT-INDI-SSASP**. La versione e il livello di rilascio sono riportati nell'intestazione di ciascuna pagina.

Al documento sono associati specifici Object Identifier (OID),

L'Object Identifier (OID) che identifica Tinexta Infocert è: 1.3.76.36.

Le policy relative ai servizi di firma elettronica qualificata remota sono le seguenti:

Descrizione	OID
Manuale-operativo- Servizio di firma remota qualificata One-time signing key	1.3.76.36.1.1.4000.1 conforme alla policy EUSPv2 0.4.0.19431.1.1.4
Manuale-operativo- Servizio di firma remota qualificata	1.3.76.36.1.1.4000.2 conforme alla policy EUSPv2 0.4.0.19431.1.1.4
Manuale-operativo- Servizio di firma remota automatica qualificata	1.3.76.36.1.1.4000.3 conforme alla policy EUSPv2 0.4.0.19431.1.1.4
Manuale-operativo- Servizio di sigillo remoto qualificato	1.3.76.36.1.1.4000.4 conforme alla policy EUSPv2 0.4.0.19431.1.1.4

Tabella 1– Policy per servizi di firma elettronica qualificati

1.3 Partecipanti e responsabilità

1.3.1 SSASP – Qualified Signature Activation Service Provider

Il Server Signature Activation Service Provider (SSASP) è il soggetto che eroga il servizio di firma elettronica qualificata remota, garantendo la generazione, custodia e attivazione delle chiavi private di firma all'interno di un dispositivo per la creazione di firma qualificata remoto (QSCD remoto).

Il servizio è erogato in conformità al Regolamento [1] e ss.mm.ii. che disciplina i requisiti di sicurezza, gestione e funzionamento dei sistemi remoti per la creazione di firme qualificate.

Tinexta Infocert S.p.A. opera quale SSASP qualificato, assicurando che:

- la coppia di chiavi per la firma sia generata in moduli crittografici certificati;
- la coppia di chiavi di firma sia generata in ambiente sicuro;
- la chiave privata non sia esportabile;
- le chiavi siano custodite nei moduli crittografici certificati;
- l'utilizzo della chiave privata sia subordinato all'autenticazione del Soggetto;
- sia garantito il controllo esclusivo del Soggetto sull'attivazione del processo di firma;
- tutte le operazioni rilevanti siano tracciate e sottoposte a misure di sicurezza e audit.

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

Denominazione sociale	**Tinexta Infocert – Società per azioni** **Società soggetta a direzione e coordinamento di Tinexta S.p.A.**
Sede legale	**Piazzale Flaminio 1/B, 00196, Roma (RM)**
Sedi operative	**Via Marco e Marcelliano n.45, 00147, Roma (RM)** **Via Fernanda Wittgens n. 2, 20123 Milano (MI)**

	Piazza Luigi da Porto n. 3, 35131 Padova (PD)
Rappresentante legale	**Danilo Cattaneo - In qualità di Amministratore Delegato**
N. di telefono	**+39 06 836691**
Partita IVA/Codice Fiscale	**07945211006**
N. Iscr. Registro Imprese	**Business Register N. 07945211006 -** *N. REA* **RM - 1064345**
Sito Web	**https://www.infocert.it**

Il SSASP opera in coordinamento con la Certification Authority per quanto riguarda l'emissione e la gestione del certificato qualificato associato alle chiavi di firma.

La Certification Authority, ai fini del presente manuale operativo può essere la stessa Infocert o un QTSP esterno.

1.3.2 Certification Authority – Autorità di certificazione

La Certification Authority (CA) è il soggetto che emette, pubblica, sospende e revoca i certificati qualificati associati alle chiavi di firma generate e custodite nel QSCD remoto. Per la disciplina di tale ruolo si rimanda al Manuale Operativo della Certification Authority.

La CA:

- verifica l'identità del Soggetto secondo le procedure previste dall'art.24 del Regolamento [1] nella sua versione vigente
- emette il certificato qualificato contenente la chiave pubblica corrispondente alla chiave privata custodita nel QSCD remoto;
- garantisce la conformità ai requisiti previsti dalla normativa vigente e dagli standard applicabili.

La CA e il SSASP operano in modo coordinato ma con ruoli distinti:

- la CA è responsabile del legame tra l'identità del soggetto e chiave pubblica;
- il SSASP è responsabile della protezione e dell'attivazione della chiave privata.

1.3.3 Registration Authority – Ufficio di Registrazione (RA)

Le Registration Authority (RA) sono soggetti delegati allo svolgimento delle attività di identificazione del Soggetto, di raccolta delle richieste relative al rilascio del certificato qualificato e di autenticazione al servizio di firma remota.

Le RA possono svolgere, tra l'altro, le seguenti attività:

- l'identificazione del Soggetto o del Richiedente,
- la registrazione dei dati del Soggetto,
- l'inoltro dei dati del Soggetto ai sistemi della CA,
- la raccolta della richiesta del certificato qualificato,

- l'attivazione della procedura di certificazione della chiave pubblica.;
- supporto nelle fasi di sospensione, revoca o rinnovo del certificato e del servizio.

Le RA operano sulla base di mandato conferito dal prestatore qualificato e nel rispetto delle procedure descritte nel presente Manuale o in quello della CA.

1.3.4 Soggetto o Firmatario

Il **Soggetto** (o Firmatario) è la persona fisica o giuridica cui sono associate:

- la coppia di chiavi di firma generate nel QSCD remoto;
- il certificato qualificato contenente la chiave pubblica corrispondente alla chiave privata di firma.

Nel contesto del servizio di firma remota, il Firmatario esercita il controllo esclusivo sulla propria chiave privata attraverso i meccanismi di autenticazione forte e attivazione previsti dal sistema.

1.3.5 Utente o Relying Party

È il soggetto che riceve un documento informatico sottoscritto con firma elettronica qualificata generata tramite il servizio remoto e che fa affidamento:

- sulla validità del certificato qualificato;
- sull'affidabilità del servizio di firma remota; sul rispetto dei requisiti di sicurezza e controllo esclusivo previsti dalla normativa applicabile.

1.3.6 Richiedente

Il Richiedente è la persona fisica o giuridica che richiede l'attivazione del servizio di firma qualificata remota per conto del Soggetto, eventualmente sostenendone i costi in qualità di Cliente del QTSP. Il ruolo, quando presente, può essere assunto anche dalla RA.

Il Richiedente può coincidere con il Soggetto, quando una persona fisica richiede il Servizio per sé stessa. In altre situazioni, il Richiedente può essere un ente o un'organizzazione, che agisce per conto di persone fisiche collegate da rapporti commerciali o nel quadro di una struttura organizzativa. Infine, può anche essere una persona fisica dotata dei poteri di rappresentanza della persona giuridica.

1.3.7 Autorità

1.3.7.1 Agenzia per l'Italia Digitale - AgID

L'Agenzia per l'Italia Digitale (**AgID**) è l'organismo di vigilanza sui prestatori di servizi fiduciari. 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].

1.3.7.2 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 [1], che è competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

1.4 Uso del certificato

1.4.1 Usi consentiti

I Il servizio di firma elettronica qualificata remota erogato da InfoCert consente al Firmatario di generare firme elettroniche qualificate mediante l'utilizzo di una chiave privata custodita in un dispositivo per la creazione di firma qualificata remoto (QSCD remoto), in conformità al Regolamento [1] e agli standard tecnici applicabili.

Il servizio può essere utilizzato esclusivamente dal Firmatario cui sono associate:

- la coppia di chiavi di firma generate nel QSCD remoto;
- il certificato qualificato contenente la corrispondente chiave pubblica;
- il mezzo di identificazione elettronica (eID means) associato al servizio.

L'utilizzo della chiave privata di firma è consentito unicamente previa autenticazione del Firmatario e attivazione del processo di firma secondo le modalità previste dal sistema, che garantiscono il controllo esclusivo della chiave da parte del Firmatario.

Le firme generate mediante il servizio sono destinate alla sottoscrizione di documenti informatici nei contesti previsti dalla normativa vigente e, congiuntamente con il certificato associato, producono gli effetti giuridici riconosciuti alla firma elettronica qualificata.

La verifica delle firme apposte tramite il servizio avviene mediante l'utilizzo del certificato qualificato associato, secondo le modalità tecniche previste dagli standard di settore.

1.4.2 Usi non consentiti

È vietato qualsiasi utilizzo del servizio di firma qualificata remota in violazione:

- delle condizioni contrattuali sottoscritte dal Soggetto;
- delle disposizioni del presente Manuale Operativo;
- dei limiti d'uso indicati nel certificato qualificato associato (key usage, extended key usage, user notice);
- delle modalità di autenticazione e attivazione previste dal sistema.

È in particolare vietato:

- tentare di accedere o attivare la chiave privata senza il rispetto delle procedure di autenticazione previste;

- utilizzare credenziali o mezzi di identificazione elettronica associati al servizio in modo improprio o non autorizzato;
- utilizzare il servizio per finalità diverse dalla generazione di firme elettroniche qualificate.

1.5 Amministrazione del manuale operativo

1.5.1 Contatti

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

Denominazione sociale	**Tinexta Infocert – Società per azioni** **Responsabile del Servizio di Firma Remota** **Via Fernanda Wittgens n. 2, 20123 Milano (MI)**
N. di telefono	**06 836691**
Contact Center	**https://help.infocert.it/contatti/ per maggiori dettagli**
Web	**https://www.firma.infocert.it, https://www.infocert.it**
E-mail	**firma.digitale@legalmail.it**

Il Soggetto o il Richiedente possono richiedere copia della documentazione a lui relativa.

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Il Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle policy, dal Responsabile della Privacy, dal Responsabile del QTSP, dal Responsabile Legale e approvato dalla Direzione Aziendale.

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale seguono le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

1.6 Definizioni e acronimi

1.6.1 Definizioni

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

Termine	*Definizione*
Conformity Assessment Body	Organismo accreditato a norma del Regolamento eIDAS come competente a

Termine	Definizione
(Organismo di valutazione della conformità) (CAB)	effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
Conformity Assessment Report (Relazione di valutazione della conformità) (CAR)	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr eIDAS [1]).
Certificato di firma elettronica	Un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona (cfr eIDAS [1]).
Certificato di sigillo elettronico	Un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona (cfr eIDAS [1]).
Certificato qualificato di firma elettronica	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (cfr eIDAS [1]).
Certificato qualificato di sigillo elettronico (QSealC)	Un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III del Regolamento eIDAS (cfr eIDAS [1]).
Chiave privata/Signing key	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]).
One Time Signing key	Chiave di firma associata, certificata, utilizzata e dismessa sulla base di una singola autorizzazione, collegata a una singola sessione di firma dei dati/documenti da firmare (DTBS/R(s))
Cliente	Soggetto con cui Infocert ha formalizzato un contratto di fornitura di servizi dietro pagamento di corrispettivo
Codice di emergenza (ERC)	Codice di sicurezza consegnato al Soggetto per inoltrare la richiesta di sospensione di un certificato sui portali del TSP.
Convalida	Il processo di verifica e conferma della validità di una firma elettronica (cfr eIDAS [1]).
Dati di convalida	Dati utilizzati per convalidare una firma elettronica (cfr eIDAS [1]).
Dati di identificazione personale	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr eIDAS [1]).
Dati per la creazione di una firma elettronica	I dati unici utilizzati dal firmatario per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica (SSCD secure system creation device)	Un software o hardware configurato utilizzato per creare una firma elettronica (cfr eIDAS [1]).
Dispositivo per la creazione di una firma elettronica qualificata QSCD)	Un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS (cfr eIDAS [1]).
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1]).
Firma automatica	Particolare procedura informatica di firma elettronica eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr eIDAS [1]).
Firma remota	Particolare procedura di firma elettronica qualificata, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse

Termine	Definizione
Firmatario	Una persona fisica che crea una firma elettronica (cfr eIDAS [1]).
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 (practice statement - PS)	Definisce le procedure che il SSASP applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr eIDAS [1]).
Online Certificate Status Protocol (OCSP)	Protocollo definito dallo IETF nella RFC 6960, consente alle applicazioni di verificare la validità del certificato in maniera più veloce e puntuale rispetto alla CRL, di cui condivide i dati.
One Time Password (OTP)	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Soggetto in un momento immediatamente antecedente all'apposizione della firma elettronica qualificata. Può essere basato su dispositivi hardware o su procedure software.
Parte facente affidamento (Utente/Relying party)	Una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario (cfr eIDAS [1]).
Prestatore di servizi fiduciari	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato (cfr eIDAS [1]).
Prestatore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr eIDAS [1]).
Prodotto	Un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari (cfr eIDAS [1]).
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: creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure creazione, verifica e convalida di certificati di autenticazione di siti web; o conservazione di firme, sigilli o certificati elettronici relativi a tali servizi (cfr eIDAS [1]).
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1]).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi (cfr eIDAS [1]).
Sigillo elettronico qualificato	Un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici (cfr eIDAS [1]).
Stato Membro	Stato Membro dell'Unione Europea
Tempo Universale Coordinato (Coordinated Universal Time)	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento (cfr eIDAS [1]).
Validazione temporale	Una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo

Termine	Definizione
elettronica qualificata	42 del Regolamento eIDAS (cfr eIDAS [1]).

Tabella 2– Definizioni

1.6.2 Acronimi e Abbreviazioni

Acronimo	Definizione
AgID	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
CA	Certification Authority
SSASP	Server Signing Application Service Provider
SSA (SSAS)	Server Signing Application (Service)
CAB	Conformity Assessment Body – Organismo di valutazione della conformità
CAD	Codice dell'Amministrazione Digitale
CAR	Conformity Assessment Report – Relazione di valutazione della conformità
CC	Common Criteria
CIE	Carta di Identità Elettronica
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguish Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smartcard, ma con superiori caratteristiche di memoria e di performance
HTTP	HyperText Transfer Protocol
IDP	Identity Provider
IETF	Internet Engineering Task Force
IR	Incaricato alla Registrazione o Registration Authority Officer
ISO	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione
ITU	International Telecommunication Union: fondata nel 1865, è l'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni
IUT	Identificativo Univoco del Titolare: è un codice associato al Soggetto che lo identifica univocamente presso la CA; il Soggetto ha codici diversi per ogni certificato in suo possesso
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati
LoA	Level of Assurance
LoIP	Level of Identity Proofing
NCA	National Competent Authority
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
OTP	OneTime Password
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number: codice associato ad un dispositivo sicuro di firma, utilizzato dal Soggetto per accedere alle funzioni del dispositivo stesso
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse,

Acronimo	Definizione
	processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto
PSD2	Payment Services Directive 2
PSP	Service Payment Provider (prestatore servizi di pagamento)
QSealC	Qualified electronic Seal Certificate
RA	Registration Authority – Autorità di Registrazione
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
RSA	Deriva dalle iniziali degli inventori dell'algoritmo: River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SPID	Sistema Pubblico di Identità Digitale
SSCD – QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una firma elettronica Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica
TIN	Tax Identification Number
UUID	Universally unique identifier
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X500	Standard ITU-T per i servizi LDAP e directory
X509	Standard ITU-T per le PKI

Tabella 5– Acronimi e abbreviazioni

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Pubblicazione e disponibilità documentazione

La documentazione afferente al servizio di Firma Remota, tra cui il presente Manuale e le condizioni generali di servizio, sono pubblicati sul sito istituzionale di Tinexta Infocert e disponibili 24 ore al giorno per 7 giorni alla settimana.

2.2 Pubblicazione delle informazioni sulla certificazione

La pubblicazione delle informazioni relative alla certificazione, allo stato dei certificati, alle CRL/OCSP e in generale agli aspetti propri della CA è disciplinata dalla documentazione della CA competente.

2.3 Periodo o frequenza di pubblicazione

2.3.1 Frequenza di pubblicazione del Manuale Operativo

Il Manuale Operativo viene pubblicato ove al paragrafo 1.5.1 con frequenza variabile quando avvengono dei cambiamenti, comunque non superiore all'anno come specificato al par. 1.5.3. Se i cambiamenti sono importanti, il SSASP 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).

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

N/A

2.4 Controllo degli accessi agli archivi pubblici

I Manuali Operativi sono pubblici, il SSASP sono liberamente accessibili in consultazione pubblica 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

Si rimanda al Certificate Policy/Certificate Practice Statement (di seguito Manuale Operativo della CA) della Certification Authority competente.

3.1.2 Necessità che il nome abbia un significato

Si rimanda al Manuale Operativo della CA

3.1.3 Anonimato e pseudonimia dei richiedenti

Si rimanda al Manuale Operativo della CA.

3.1.4 Regole di interpretazione dei tipi di nomi

Si rimanda al Manuale Operativo della CA.

3.1.5 Univocità dei nomi

Si rimanda al Manuale Operativo della CA.

3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

Si rimanda al Manuale Operativo della CA.

3.2 Convalida iniziale dell'identità

L'attivazione del servizio di firma elettronica qualificata remota è subordinata alla preventiva identificazione del Soggetto secondo le modalità previste per l'emissione del certificato qualificato.

Le attività di identificazione sono svolte dalla Certification Authority e/o dalla Registration Authority. Il SSASP si basa su tali verifiche per procedere alla generazione della coppia di chiavi nel QSCD remoto e per associare il servizio al Firmatario.

3.2.1 Metodo per dimostrare il possesso della chiave privata

Nel servizio di firma qualificata remota la coppia di chiavi crittografiche associata al certificato qualificato è generata all'interno del dispositivo per la creazione di firma qualificata remoto (QSCD remoto), in ambiente sicuro e con modalità tali da garantire che la chiave privata non sia esportabile.

La dimostrazione del possesso della chiave privata (Proof of Possession) associata alla chiave pubblica da certificare è assicurata dal processo di generazione della coppia di chiavi all'interno

del QSCD remoto e dal collegamento tra tale processo e la richiesta di emissione del certificato qualificato attraverso la sottoscrizione di una CSR con la chiave privata generata.

Le modalità con cui la Certification Authority verifica la Proof of Possession ai fini dell'emissione del certificato qualificato sono disciplinate nel Manuale Operativo della CA.

Il presente Manuale Operativo non disciplina nel dettaglio le procedure di verifica della Proof of Possession effettuate dalla Certification Authority.

3.2.2 Autenticazione dell'identità della persona giuridica

Nel caso di certificati riferiti a persone giuridiche, l'attivazione del servizio avviene nei confronti di una persona fisica identificata che agisce quale rappresentante o soggetto autorizzato.

Il SSASP, dopo le verifiche effettuate dalla CA/RA in merito ai poteri di rappresentanza, associa la chiave privata custodita nel QSCD remoto alla persona fisica autorizzata all'attivazione del sigillo.

3.2.3 Autenticazione dell'identità della persona fisica

L'autenticazione dell'identità della persona fisica ai fini del rilascio del certificato qualificato associato al servizio di firma remota è effettuata secondo le procedure stabilite dalla Certification Authority e, ove applicabile, dalle Registration Authority (RA) delegate.

3.2.4 Informazioni del Soggetto o del Richiedente non verificate

Il SSASP non effettua verifiche autonome sugli attributi inseriti nel certificato qualificato. Eventuali informazioni non verificate rientrano nella responsabilità della Certification Authority secondo le proprie policy.

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

Nel contesto del servizio di firma qualificata remota, l'identificazione del Soggetto ai fini dell'emissione del certificato qualificato è effettuata secondo le procedure stabilite dalla Certification Authority.

Il SSASP è invece responsabile dell'autenticazione del Soggetto ai fini dell'utilizzo della chiave privata custodita nel QSCD remoto e dell'attivazione del processo di firma.

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

Nel contesto del servizio di firma qualificata remota, qualora sia prevista la generazione di una nuova coppia di chiavi all'interno del QSCD remoto in occasione del rinnovo o della riemissione del certificato qualificato, l'identificazione del Soggetto ai fini del rilascio del nuovo certificato è effettuata secondo le procedure stabilite dalla Certification Authority.

Il SSASP è responsabile dell'autenticazione del Soggetto per l'accesso al servizio e per l'utilizzo

della chiave privata custodita nel QSCD remoto. Prima che il Soggetto possa utilizzare la nuova chiave privata per la generazione di firme elettroniche qualificate, il sistema richiede l'autenticazione del Soggetto mediante i meccanismi previsti dal servizio.

Tali meccanismi di autenticazione sono progettati in modo da garantire che solo il Soggetto legittimo possa attivare il processo di firma e che l'utilizzo della chiave privata avvenga sotto il suo controllo esclusivo, in conformità ai requisiti di sicurezza previsti dalla normativa applicabile e dagli standard tecnici di riferimento.

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

Nel caso di riemissione di un certificato qualificato con generazione di una nuova coppia di chiavi a seguito della revoca del certificato precedente, l'identificazione del Soggetto ai fini dell'emissione del nuovo certificato è effettuata secondo le procedure stabilite dalla Certification Authority.

Nel servizio di firma qualificata remota, la nuova coppia di chiavi è generata all'interno del QSCD remoto. L'utilizzo della chiave privata per la generazione delle firme è consentito esclusivamente previa autenticazione del Soggetto secondo i meccanismi previsti dal servizio e gestiti dal SSASP.

3.3.3 Identificazione e autenticazione di un Soggetto per il rinnovo dei certificati

Nel caso di rinnovo di un certificato qualificato, l'identificazione del Soggetto ai fini del rilascio del nuovo certificato è effettuata secondo le procedure stabilite dalla Certification Authority, e la richiesta di rinnovo viene firmata con la chiave privata corrente.

3.4 Identificazione e autenticazione per le richieste di revoca o sospensione

Le richieste di revoca o sospensione dei certificati qualificati associati al servizio di firma remota sono gestite dalla Certification Authority, secondo le procedure descritte nella relativa Certification Policy (CP) e nel Certification Practice Statement (CPS).

A seguito della revoca di un certificato qualificato associato al servizio di firma remota, il SSASP provvede alla distruzione della chiave privata corrispondente custodita nel QSCD remoto, secondo le procedure di sicurezza previste dal servizio.

Il presente Manuale Operativo non disciplina nel dettaglio le procedure operative di revoca o sospensione dei certificati, che rientrano nel ciclo di vita del certificato gestito dalla Certification Authority.

3.4.1 Richiesta da parte del Soggetto

n/a

3.4.2 Richiesta da parte del Richiedente

n/a

4 OPERATIVITÁ

4.1 Richiesta e attivazione del servizio

4.1.1 Chi può richiedere il servizio

Il servizio di firma elettronica qualificata remota può essere richiesto dal Firmatario oppure da un Richiedente legittimato a richiedere il servizio per conto del Firmatario o ad assumersene i costi, nei limiti previsti dalla documentazione contrattuale. L'attivazione può avvenire tramite i canali messi a disposizione da Infocert e/o tramite Registration Authority autorizzate.

Nel caso di persone giuridiche, la richiesta è presentata da una persona fisica identificata che agisce quale legale rappresentante o soggetto munito di procura, secondo le procedure previste.

4.1.2 Processo di Attivazione e responsabilità

Il processo di registrazione e attivazione del servizio di firma elettronica qualificata remota prevede:

- l'identificazione del Firmatario secondo le procedure della Certification Authority e/o della Registration Authority;
- la generazione della coppia di chiavi all'interno del QSCD remoto;
- l'emissione del certificato qualificato da parte della CA associato alla chiave pubblica;
- l'associazione tra identità del Firmatario, certificato qualificato, chiave privata e mezzi di autenticazione abilitati all'attivazione della firma.

Il SSASP è responsabile della corretta generazione e custodia della chiave privata nel QSCD remoto, nonché della configurazione dei meccanismi di attivazione della firma in modo da garantire il controllo esclusivo del Firmatario.

La CA è responsabile della verifica dell'identità del Soggetto e dell'emissione del certificato qualificato secondo le proprie policy.

L'attivazione del servizio si considera completata quando il Firmatario è posto nelle condizioni di autenticarsi e di generare firme elettroniche qualificate tramite il QSCD remoto, nel rispetto delle regole del servizio.

4.2 Elaborazione della richiesta

4.2.1 Esecuzione delle funzioni di identificazione e autenticazione

L'identificazione del Soggetto ai fini dell'emissione del certificato qualificato è effettuata secondo le procedure della Certification Authority e/o della Registration Authority. L'autenticazione del Soggetto ai fini dell'utilizzo della chiave privata custodita nel QSCD remoto

e dell'attivazione del processo di firma è invece effettuata dal SSASP, secondo le modalità previste dal servizio. Il SSASP utilizza sistemi di autenticazione a due fattori non basati necessariamente su certificati digitali, le cui chiavi private sono custodite su dispositivi che soddisfano i requisiti di cui all'Allegato II del Regolamento [1] e del Parlamento Europeo e del Consiglio. Tale livello corrisponde al Level of Assurance LoA3 dello standard ISO/IEC 29115 (Substantial). A questo livello sono rilasciate al Firmatario un identificativo utente, una password e dei sistemi OTP (One-Time Password), gestiti tramite protocollo SMS e/o applicazioni, che assicurano il soddisfacimento dei requisiti previsti dalla normativa. Possono essere utilizzati anche sistemi biometrici di accesso, nel rispetto delle previsioni del Garante per la Protezione dei Dati Personali.

Sulla base del processo configurato, Infocert può rendere disponibile al Firmatario i seguenti metodi di autenticazione:

A. One Time Password via SMS

B. Time Based One Time Password

C. Autenticazione implicita con QR code

D. Autenticazione implicita push notification

E. TOTP tramite dispositivo hardware

F. Asserzione di autorizzazione.

4.2.1.1 Persona fisica

Nel caso di persona fisica, l'identificazione è svolta dalla CA/RA o da un IPSP incaricato.

Il SSASP, ricevuto l'esito positivo del processo di identificazione, genera la coppia di chiavi nel QSCD remoto e associa il servizio al Soggetto.

4.2.1.2 Persona giuridica

Nel caso di persona giuridica, l'identificazione della persona fisica autorizzata è svolta dalla CA/RA.

Il SSASP associa il servizio alla persona fisica autorizzata, garantendo che l'attivazione della chiave privata sia subordinata alla sua autenticazione.

Le verifiche sui poteri di rappresentanza sono di competenza della CA.

4.2.1.3 Registrazione

A seguito della richiesta del servizio di firma elettronica qualificata remota, il SSASP crea un'utenza nei propri sistemi associata al servizio di firma remota richiesto.

L'utenza è utilizzata per la gestione operativa del servizio e per l'associazione tra:

- il Soggetto titolare del servizio;

- il servizio di firma remota attivato;
- la coppia di chiavi generata nel QSCD remoto;
- il certificato qualificato emesso dalla Certification Authority;
- i mezzi di autenticazione utilizzati per l'attivazione della firma.

La creazione dell'utenza avviene prima dell'emissione del certificato qualificato, che è richiesta successivamente dal SSASP alla Certification Authority, anche qualora questa sia diversa dal prestatore del servizio di firma remota, attraverso la sottoscrizione di una CSR con la chiave privata del Soggetto.

4.2.2 Approvazione o rifiuto della richiesta del Servizio

La richiesta di attivazione del servizio di firma elettronica qualificata remota è valutata sulla base dell'esito delle verifiche di identificazione del Soggetto e della correttezza delle informazioni fornite.

In caso di esito positivo delle verifiche svolte dalla CA, il SSASP procede con l'attivazione del servizio, la generazione della coppia di chiavi nel QSCD remoto e la richiesta di emissione del certificato qualificato alla Certification Authority.

Qualora le verifiche non abbiano esito positivo o risultino incomplete, la richiesta può essere rifiutata o sospesa fino alla risoluzione delle eventuali anomalie.

L'emissione del certificato qualificato resta in ogni caso di competenza della Certification Authority, in conformità alle proprie policy e procedure.

4.2.3 Tempo massimo per l'elaborazione della richiesta del certificato

Il tempo necessario per l'elaborazione della richiesta di attivazione del servizio di firma elettronica qualificata remota dipende dal completamento delle attività di identificazione del Soggetto, dalla verifica delle informazioni fornite e dalla disponibilità dei dati necessari all'attivazione del servizio.

Una volta completate tali verifiche dalla CA, il SSASP procede alla generazione della coppia di chiavi nel QSCD remoto e alla richiesta di emissione del certificato qualificato alla Certification Authority.

I tempi di emissione del certificato qualificato sono determinati dalle procedure operative della Certification Authority.

4.3 Generazione e attivazione della chiave nel QSCD

4.3.1 Operatività del SSASP per la generazione o gestione della chiave

4.3.1.1 Generazione della coppia di chiavi nel QSCD

La coppia di chiavi crittografiche utilizzata per il servizio di firma elettronica qualificata remota è generata all'interno del QSCD, in un ambiente sicuro gestito dal SSASP.

La generazione delle chiavi avviene mediante moduli crittografici conformi ai requisiti applicabili ai dispositivi per la creazione di firma qualificata. La chiave privata non è esportabile ed è custodita all'interno del QSCD per tutta la durata del servizio.

La chiave pubblica corrispondente è utilizzata dal SSASP per richiedere alla Certification Authority l'emissione del certificato qualificato associato al Soggetto.

La chiave privata può essere utilizzata esclusivamente tramite i meccanismi di attivazione della firma previsti dal servizio e sotto il controllo esclusivo del Soggetto.

4.3.1.2 Tipologie di chiavi nel servizio di firma remota

Nel servizio di firma elettronica remota sono previste diverse tipologie di chiavi, in funzione del modello operativo del servizio.

In particolare, il servizio può prevedere:

- chiavi persistenti, associate stabilmente al Soggetto e utilizzate per la generazione di firme nel corso della validità del certificato qualificato;
- chiavi one-time, generate per la sottoscrizione di una singola operazione di firma;
- chiavi utilizzate nell'ambito di processi di firma automatica, attivate secondo le modalità previste dal servizio
- chiavi utilizzate per la generazione di sigilli.

In tutti i casi, le chiavi private sono generate e custodite nel QSCD remoto e il loro utilizzo è consentito esclusivamente a seguito dell'autenticazione del Soggetto secondo una delle modalità sopracitate o eventualmente fornite dalla RA, e dell'attivazione del processo di firma tramite i sistemi del servizio configurato.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

L'emissione del certificato qualificato è di competenza della Certification Authority che notifica al Richiedente le informazioni per l'utilizzo dello stesso secondo le policy proprie della CA.

4.3.3 Attivazione

4.3.3.1 Attivazione operativa delle chiavi

A seguito della conferma dell'emissione del certificato qualificato, il SSASP procede all'attivazione operativa della chiave privata custodita nel QSCD remoto.

L'attivazione operativa consiste nell'associazione della chiave privata con:

- il certificato qualificato emesso dalla Certification Authority;
- i mezzi di autenticazione abilitati all'attivazione della firma.

A partire da tale momento, la chiave privata può essere utilizzata per la generazione di firme elettroniche qualificate tramite il servizio di firma remota, previa autenticazione di livello almeno substantial del Firmatario secondo le modalità previste dal servizio.

L'utilizzo della chiave privata per generare una firma qualificata avviene esclusivamente tramite il processo di Signature Activation.

Per ogni operazione di firma:

- il Firmatario attiva il processo di firma con le proprie credenziali;
- vengono generati e validati i Signature Activation Data (SAD);
- il QSCD verifica la validità del SAD e lo stato della chiave

Solo in caso di esito positivo la chiave privata è utilizzata per generare la firma o il sigillo.

4.3.3.2 Associazione del certificato alle chiavi

La chiave privata generata nel QSCD remoto è associata al certificato qualificato emesso dalla Certification Authority tramite la corrispondente chiave pubblica.

Il SSASP verifica, prima di consentire l'attivazione della firma, che il certificato associato sia valido e non risulti sospeso o revocato secondo le informazioni messe a disposizione dalla CA.

La gestione dello stato del certificato rimane di competenza della Certification Authority, mentre il SSASP è responsabile dell'inibizione dell'attivazione della chiave in caso di certificato non valido.

4.4 Autorizzazione della operazione di firma

4.4.1 Comportamenti concludenti di autorizzazione dell'operazione di firma

La Richiesta dell'operazione di firma si considera effettuata quando il Firmatario, a seguito dell'autenticazione al servizio, autorizza esplicitamente l'utilizzo della chiave privata custodita nel QSCD remoto per la generazione della firma.

Costituiscono comportamenti concludenti di richiesta dell'operazione di firma:

- l'autenticazione del Firmatario mediante i mezzi di autenticazione associati al servizio.
- la manifestazione esplicita di autorizzazione (consenso) dell'operazione di firma tramite i meccanismi previsti dal sistema.

A seguito di tali operazioni, il sistema procede all'attivazione della chiave privata nel QSCD remoto e alla generazione della firma elettronica qualificata, garantendo che l'utilizzo della chiave privata avvenga sotto il controllo esclusivo del Firmatario.

4.4.2 Produzione delle firme

A seguito dell'autenticazione del Firmatario e dell'autorizzazione dell'operazione di firma secondo le modalità previste dal servizio, il sistema procede all'utilizzo della chiave privata custodita nel QSCD per la generazione della firma elettronica qualificata che viene restituita al processo richiedente.

Il SSASP garantisce la tracciabilità tecnica dell'operazione di firma nei propri sistemi, nel rispetto delle normative e degli standard applicabili.

4.4.3 Notifica dell'avvenuta esecuzione dell'operazione di firma

Viene resa disponibile al Soggetto della avvenuta esecuzione dell'operazione di firma con il riferimento temporale della stessa.

4.5 Uso della coppia di chiavi e del certificato

4.5.1 Uso della chiave privata da parte del Soggetto

Nel servizio di firma elettronica qualificata remota, la chiave privata è custodita nel QSCD e non è nella disponibilità materiale del Firmatario.

Il Firmatario è responsabile:

- della corretta custodia e protezione dei mezzi di autenticazione associati al servizio;
- della segretezza dei codici o fattori di autenticazione utilizzati per l'attivazione della firma;
- dell'utilizzo del servizio esclusivamente per le finalità consentite dal contratto e dalla normativa applicabile.

Il Soggetto non deve:

- consentire a terzi l'utilizzo dei propri mezzi di autenticazione;
- richiedere o autorizzare operazioni di firma in assenza di volontà consapevole;
- utilizzare il servizio qualora ritenga compromessi i propri mezzi di autenticazione.

L'utilizzo della chiave privata avviene esclusivamente tramite il processo di attivazione della firma previsto dal servizio, a seguito di autenticazione e della generazione e validazione dei Signature Activation Data (SAD).

Eventuali limiti d'uso inseriti nel certificato qualificato sono di competenza della Certification Authority e devono essere rispettati dal Firmatario.

4.5.2 Uso della chiave pubblica e verifica della firma da parte degli Utenti Finali

Il soggetto che riceve un documento sottoscritto mediante il servizio di firma remota deve:

- verificare la validità della firma elettronica qualificata;
- verificare lo stato del certificato qualificato (non scaduto, non revocato, non sospeso) tramite i servizi messi a disposizione dalla Certification Authority;
- verificare eventuali limitazioni d'uso o di valore riportate nel certificato.

La verifica della firma e del certificato rientra nella responsabilità del soggetto che fa affidamento sulla firma stessa.

4.5.3 Limiti d'uso del servizio e del certificato

L'utilizzo del servizio di firma remota e del certificato qualificato è soggetto alle condizioni contrattuali del servizio e alle eventuali limitazioni indicate nel certificato qualificato.

4.6 Rinnovo

Il rinnovo del certificato qualificato associato al servizio di firma remota è effettuato dalla Certification Authority secondo le proprie politiche e pratiche.

Il Titolare del Certificato invia alla Certification Authority la richiesta di rinnovo, a fronte della quale viene creata una nuova copia di chiavi, una richiesta di certificato con gli stessi dati del certificato precedente e firmata con il certificato precedente.

Il SSASP mantiene attiva l'associazione tra il certificato rinnovato e i meccanismi di autenticazione e genera una nuova coppia di chiavi da associare al certificato rinnovato.

4.6.1 Motivi per il rinnovo

I motivi di rinnovo sono regolati dalle politiche e pratiche della CA.

4.6.2 Chi può richiedere il rinnovo

Il rinnovo del certificato può essere richiesto dal Titolare, secondo le politiche e pratiche della Certification Authority.

4.6.3 Elaborazione della richiesta di rinnovo del certificato

Il rinnovo viene richiesto alla CA tramite il servizio di Firma, il quale si occuperà di generare la nuova coppia di chiavi per richiedere alla CA l'emissione del nuovo certificato.

4.7 Riemissione con nuove chiavi

La riemissione del certificato con generazione di una nuova coppia di chiavi (re-key) consente

al Soggetto già identificato di ottenere un nuovo certificato qualificato associato a una diversa coppia di chiavi.

4.7.1 Motivi per la riemissione con nuove chiavi

La riemissione del certificato con una nuova chiave (re-key) consente ad un Soggetto già identificato e in possesso di un certificato, di certificare una diversa coppia di chiavi, mantenendo gli stessi dati identificativi. La data di scadenza del nuovo certificato è definita contrattualmente.

Esempi, non esaustivi, possono essere la ri-certificazione di una nuova coppia di chiavi su dispositivo remoto in prossimità della scadenza del certificato o su un dispositivo in dismissione, o la sostituzione di chiavi crittografiche deboli con chiavi crittografiche generate con algoritmi più robusti.

La procedura si applica esclusivamente a certificati emessi da Infocert.

4.7.2 Chi può richiedere la riemissione con nuove chiavi

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

4.7.3 Elaborazione della richiesta di riemissione con nuove chiavi

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

4.8 Modifica del certificato

n/a

4.9 Revoca e sospensione del certificato

La revoca o sospensione del certificato qualificato è di esclusiva competenza della Certification Authority.

Il SSASP, ricevuta notifica della revoca o sospensione, impedisce l'utilizzo della chiave privata nel QSCD remoto, e nel caso della revoca procede alla distruzione della chiave stessa.

4.10 Servizi riguardanti lo stato del certificato

N/A

4.11 Disdetta dai servizi del SSASP

La cessazione del servizio di firma remota comporta l'inibizione dell'utilizzo della chiave privata e la sua distruzione nel QSCD secondo procedure controllate e tracciate.

La distruzione assicura che eventuali copie o informazioni residue non possano essere utilizzate per ricostruire la chiave.

4.12 Deposito presso terzi e recovery della chiave

Non è previsto deposito della chiave privata (signing key) presso terzi esterni all'infrastruttura del QSCD remoto.

Il servizio prevede meccanismi di backup della signing key nell'ambito dell'infrastruttura del QSCD remoto, al fine di garantire la continuità del servizio.

Tutte le chiavi private, incluse le signing key, le chiavi di infrastruttura e le chiavi di controllo, sono conservate esclusivamente in forma protetta e non sono mai memorizzate in stato non protetto.

Qualora una chiave privata sia esportata dal QSCD remoto per finalità di backup, essa è protetta in modo da garantire confidenzialità e integrità con un livello di sicurezza almeno equivalente a quello garantito all'interno del QSCD; sono utilizzati esclusivamente algoritmi e parametri crittografici di robustezza equivalente o superiore.

Le operazioni di backup, conservazione e ripristino delle chiavi sono eseguite esclusivamente da personale autorizzato. Le master key utilizzate per la protezione delle chiavi utente e delle chiavi operative sono oggetto di backup, conservazione e ripristino sotto controllo multiplo (almeno dual control) e sono detenute al di fuori del QSCD esclusivamente in forma protetta.

Il numero di copie dei dataset contenenti chiavi è limitato al minimo necessario a garantire la continuità operativa del servizio.

5 MISURE DI SICUREZZA E CONTROLLI

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

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

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

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

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

5.1 Sicurezza fisica

Per l'erogazione dei servizi oggetto del presente documento, Tinexta Infocert si appoggia a cloud pubblici e infrastrutture cloud private sul territorio italiano.

Gli accessi ai Data Center sono regolati dalle procedure Infocert di sicurezza. All'interno dei Data Center che ospitano le Certification Authority e alcune componenti del servizio SSASP, quali il SAM (Signature Activation Module) e il modulo crittografico, sono previste delle High Security Trusted Zone (HSTZ) per l'accesso alle quali sono previste misure di sicurezza aggiuntive e specifiche autorizzazioni.

5.1.1 Smaltimento dei rifiuti

Infocert adotta un sistema di gestione certificato ISO 14001 per la gestione ambientale sostenibile.

L'organizzazione adotta procedure interne per la cancellazione sicura dei dati sui propri dispositivi HSM tramite l'utilizzo di fornitori che ne garantiscono la cancellazione sicura.

Adotta inoltre un ciclo di gestione dei rifiuti conforme alle normative nazionali vigenti tramite procedure per la gestione e il monitoraggio del ciclo di vita dei rifiuti e si avvale esclusivamente di fornitori autorizzati al trasporto e al destino degli stessi.

5.2 Controlli procedurali

5.2.1 Ruoli chiave

I ruoli chiave sono coperti da figure dotate dei necessari requisiti di esperienza, professionalità e competenza tecnica e giuridica, che vengono continuamente verificati mediante le valutazioni annuali.

La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

5.3 Controllo del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

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

5.3.2 Procedure di controllo delle esperienze pregresse

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

5.3.3 Requisiti di formazione

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

5.3.4 Frequenza di aggiornamento della formazione

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

- Incontro con la Direzione Aziendale per la raccolta dei dati relativi alle esigenze formative necessarie per raggiungere gli obiettivi aziendali;
- Intervista ai Responsabili per la rilevazione delle esigenze formative specifiche delle

proprie aree;
- Restituzione dei dati raccolti alla Direzione Aziendale per chiusura ed approvazione del Piano Formativo.

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

5.3.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.

Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 (dieci) giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.

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

5.3.6 Sanzioni per azioni non autorizzate

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

5.3.7 Controlli sul personale non dipendente

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

5.3.8 Documentazione che il personale deve fornire

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette Infocert.

5.4 Gestione degli eventi del QTSP

Gli eventi legati alla gestione del SSAS e della vita delle chiavi sono raccolti mediante le modalità previste dai sistemi di Conservazione a norma e descritte nel relativo manuale della sicurezza.

5.4.1 Tipi di eventi memorizzati

Sono registrati:

- eventi di sicurezza, avviamento, spegnimento, crash di sistema e guasti hardware dei sistemi SSASP;
- eventi relativi alla gestione delle signing key nel QSCD remoto (generazione, attivazione, distruzione, eventuale backup e ripristino);

- eventi relativi alla gestione delle sessioni di firma e alla validazione dei Signature Activation Data (SAD);
- eventi di autenticazione del Soggetto;
- accessi logici alle applicazioni del SSASP;
- accessi fisici ai locali ad alta sicurezza dove risiedono i sistemi del QSCD remoto.

Per quanto riguarda identificazione del Soggetto ed emissione del certificato, i relativi log sono gestiti dalla Certification Authority.

Ogni evento è registrato con data e ora di sistema.

5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo

Il trattamento e raggruppamento dei dati nonché memorizzazione sui servizi Infocert di Conservazione a norma si conclude con frequenza definita dalle pratiche del SSASP.

5.4.3 Periodo di conservazione degli eventi del SSAS

I log del SSASP sono conservati per un periodo conforme ai requisiti normativi applicabili ai servizi fiduciari qualificati.

Nel caso in cui il QTSP sia Infocert, il periodo di conservazione è di almeno 20 anni dalla scadenza del certificato, fino ad un massimo di 23 anni dalla data di emissione.

5.4.4 Notifica in caso di identificazione di vulnerabilità

Eventuali vulnerabilità rilevanti sono gestite nell'ambito del sistema di gestione della sicurezza delle informazioni del SSASP e trattate secondo le procedure di gestione degli incidenti.

5.4.5 Valutazioni di vulnerabilità

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

5.5 Archiviazione dei verbali

5.5.1 Tipi di verbali archiviati

Vengono redatti e archiviati verbali relativi ai più importanti eventi di SSAS. I verbali vengono conservati per 20 anni dal SSASP a mezzo dei servizi Infocert di Conservazione a norma dei documenti informatici.

5.5.2 Protezione dei verbali

La protezione è garantita dai servizi Infocert di Conservazione a norma dei documenti

informatici.

5.5.3 Procedure di backup dei verbali

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

5.5.4 Requisiti per la marcatura temporale dei verbali

n/a

5.5.5 Sistema di memorizzazione degli archivi

La raccolta dei verbali avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dai servizi Infocert di Conservazione a norma dei documenti informatici e descritti nel manuale della sicurezza.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

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

5.6 Disaster recovery

5.6.1 Procedure per la gestione degli incidenti

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

5.6.2 Corruzione delle macchine, del software o dei dati

In caso di guasto del dispositivo sicuro di firma HSM contenente le chiavi di firma si fa ricorso alla copia di backup delle chiavi di firma 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.

5.6.3 Erogazione dei servizi di SSASP 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 secondo le Policy di Sicurezza.

5.7 Cessazione del servizio della SSASP

In caso di cessazione del servizio di firma elettronica qualificata remota, il SSASP ne dà comunicazione all'Autorità di vigilanza nei termini previsti dalla normativa applicabile e informa i Firmatari, i Richiedenti e gli eventuali soggetti contrattualmente coinvolti delle procedure previste dal Termination Plan.

6 CONTROLLI DI SICUREZZA TECNOLOGICA

6.1.1 Generazione della coppia di chiavi Generazione della coppia di chiavi del Soggetto

Le chiavi asimmetriche sono generate all'interno di un Dispositivo Sicuro per la Creazione della Firma QSCD di tipo HSM utilizzando le funzionalità native offerte dal dispositivo stesso.

6.1.2 Consegna della chiave privata al Soggetto

La chiave privata è contenuta esclusivamente nel dispositivo crittografico.

6.1.3 Consegna della chiave pubblica alla CA

La chiave pubblica è trasmessa alla Certification Authority per l'emissione del certificato qualificato secondo procedure sicure e tracciate da parte del SSASP.

6.1.4 Consegna della chiave pubblica agli utenti

N/A

6.1.5 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware remoto di cui sopra.

Le emissioni delle chiavi del soggetto possono avvenire secondo le seguenti specifiche:

1) chiavi asimmetriche EC su una delle curve ellittiche previste dal documento Agreed Cryptographic Mechanisms" (meccanismi crittografici concordati) pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) di lunghezza non inferiore a 256 bit.

   - BrainpoolP256r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7)}
   - BrainpoolP384r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP384r1(11)}
   - BrainpoolP512r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP512r1(13)}
   - Secp256r1: {iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}
   - Secp384r1: {iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}
   - Secp521r1: {iso(1) identified-organization(3) certicom(132) curve(0) ansip521r1(35)}

2) chiavi asimmetriche RSA con lunghezza non inferiore a 3072 bits.

6.1.6 Controlli di qualità e generazione della chiave pubblica

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

6.1.7 Scopo di utilizzo della chiave

6.1.7.1 Utilizzo chiave di CA

n/a

6.1.7.2 Utilizzo chiave del Soggetto

Lo scopo di utilizzo della chiave del Soggetto è determinato dall'estensione KeyUsage come definita nello standard X509. Le estensioni sono regolate dalla CA.

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 firma remota e automatica del Soggetto sono presenti nella lista dei QSCD notificati come definito nel Regolamento [1]:

- TRISS Trust Remote InfoCert Signing Server version 1.0.2,
- Qualified Signature and Seal Creation Device (QSCD) Intesi PkBox, version 3.4.

6.2.2 Controllo di più persone della chiave privata

Le operazioni critiche sulle chiavi (backup, ripristino, distruzione, gestione master key) sono soggette a controllo multiplo (dual control).

6.2.3 Deposito presso terzi della chiave privata di CA

n/a

6.2.4 Backup della chiave privata

Il backup della signing key è effettuato in forma protetta con livello di sicurezza equivalente o superiore a quello del QSCD.

Le operazioni sono eseguite esclusivamente da personale autorizzato e le master key sono gestite sotto controllo multiplo.

Il numero di copie è limitato al minimo necessario alla continuità del servizio.

6.2.5 Archiviazione della chiave privata

Non è prevista archiviazione della signing key al di fuori dei meccanismi di backup disciplinati.

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

Qualora la chiave sia trasferita tra moduli crittografici per esigenze di continuità del servizio, il trasferimento avviene in forma cifrata e protetta con livello di sicurezza equivalente

6.2.7 Memorizzazione della chiave privata su modulo crittografico

La chiave di certificazione viene generata e memorizzata in un'area protetta del dispositivo crittografico, gestito dal SSASP, 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

N/A

6.2.9 Metodo di disattivazione della chiave privata

La signing key è automaticamente disattivata al termine della sessione di firma

6.2.10 Metodo per distruggere la chiave privata

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.

6.3 Altri aspetti della gestione delle chiavi

n/a

6.3.1 Archiviazione della chiave pubblica

n/a

6.3.2 Periodo di validità del certificato e della coppia di chiavi

Il periodo di validità del certificato e delle tipologie di chiavi, così come descritte al paragrafo 4.3.1.2 è determinato sulla base:

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

A tal fine, Tinexta InfoCert adotta parametri crittografici coerenti con gli standard di riferimento e con le più recenti indicazioni a livello europeo, incluse le raccomandazioni dell'European Cybersecurity Certification Group (ECCG) pubblicate da ENISA in materia di meccanismi crittografici.
La durata delle chiavi è limitata dalla durata del certificato come da politiche e pratiche definite

dalla CA.

6.4 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.3.3 e 6.3.

6.5 Controlli sulla sicurezza informatica

6.5.1 Requisiti di sicurezza specifici dei computer

I sistemi operativi degli elaboratori utilizzati nelle attività da SSASP per la generazione delle chiavi, sono securizzati (hardening), sono cioè configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della SSAS.

L'accesso da parte degli Amministratori di sistema, a tale scopo 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 secondo le policy di sicurezza del SSASP

6.6 Operatività sui sistemi di controllo

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

Nel SGSI sono previsti procedure e controlli per:

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

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

6.7 Controlli di sicurezza della rete

Infocert ha progettato, per il servizio di firma remota qualificata, un'infrastruttura di sicurezza di rete basata su meccanismi di segregazione logica e fisica, firewall multilivello e utilizzo di protocolli crittografici sicuri, al fine di proteggere:

- le comunicazioni tra l'SSAS e sistemi della CA;
- le comunicazioni tra SSAS e il QSCD remoto;
- le comunicazioni tra le applicazioni che invocano il servizio di firma e l'SSAS;
- le comunicazioni tra amministratori/operatori e l'SSAS.

Le comunicazioni avvengono esclusivamente tramite canali cifrati mediante protocolli sicuri conformi allo stato dell'arte (es. TLS), al fine di garantire confidenzialità e integrità dei dati scambiati, inclusi i dati di attivazione della firma.

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).

7 FORMATO DELLE CHIAVI

7.1 Algoritmi di Firma supportati

Cryptographic Operation	Algorithm	Key Sizes	Padding	Hash Algorithm	Applicable Standards
Digital signature generation	RSA PKCS#1 v1.5	3072-bit to 4096-bit	RSASSAPKCS1-v1.5	SHA256 SHA384 SHA512 SHA3-256 SHA3-384 SHA3-512	IETF RFC 3447
Digital signature generation	RSA PKCS#1 PSS	3072-bit to 4096-bit	RSASSA-PSS	SHA256 SHA384 SHA512	IETF RFC 3447
Digital signature generation	ECDSA BrainpoolP256r1	256-bit	Not Applicable	SHA-256 SHA3-256	SOGIS v1.2
Digital signature generation	ECDSA BrainpoolP320r1	320-bit	Not Applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA BrainpoolP384r1	384-bit	Not Applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA BrainpoolP512r1	512-bit	Not Applicable	SHA-512 SHA3-512	SOGIS v1.2
Digital signature generation	ECDSA Secp256r1	256-bit	Not Applicable	SHA-256 SHA3-256	SOGIS v1.2
Digital signature generation	ECDSA Secp384r1	384-bit	Not Applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA Secp521r1	521-bit	Not Applicable	SHA-512 SHA3-512	SOGIS v1.2

8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e no, in conformità al Regolamento [1] è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento.

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

8.1 Frequenza o circostanze per la valutazione di conformità

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

8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

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

8.3 Rapporti tra Infocert e CAB

Infocert presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento [1], sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403 e UNI CEI EN ISO/IEC 17065:2012.

8.4 Aspetti oggetto di valutazione

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

8.5 Azioni in caso di non conformità

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

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

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

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

I costi del Servizio di firma remota dipendono dalla configurazione richiesta, in base a tariffe definite dal contratto di servizi tra il Cliente e Infocert.

Negli altri casi, le tariffe sono disponibili presso i siti https://www.firma.infocert.it/ e http://ecommerce.infocert.it.

Il SSASP può stipulare accordi commerciali con le CA le RA, e/o i Clienti prevedendo tariffe specifiche.

9.1.2 Tariffe per l'accesso ai certificati

n/a.

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

n/a.

9.1.4 Tariffe per altri servizi

Le tariffe sono disponibili presso i siti https://www.firma.infocert.it/ e http://ecommerce.infocert.it.

9.1.5 Politiche per il rimborso

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

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Infocert ha stipulato idonea polizza assicurativa per la copertura dei rischi dell'attività e dei danni causati a terzi, come previsto dalla determinazione AgID n. 185/2017. La polizza prevede i seguenti massimali:

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

9.2.2 Altre attività

n/a

9.2.3 Garanzia o copertura assicurativa per i soggetti finali

Si veda il paragrafo 9.2.1.

9.3 Confidenzialità delle informazioni di business

9.3.1 Ambito di applicazione delle informazioni confidenziali

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

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

n/a

9.3.3 Responsabilità di protezione delle informazioni confidenziali

n/a

9.4 Privacy

Le informazioni relative al Soggetto e al Richiedente di cui il SSASP 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). In particolare, i dati personali vengono trattati da Infocert in conformità a quanto indicato nel Codice dell'Amministrazione Digitale, nel Decreto Legislativo 30 giugno 2003, n. 196 e nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018.

9.4.1 Programma sulla privacy

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

9.4.2 Dati che sono trattati come personali

Sono trattati come dati personali i dati che ricadono nella corrispondente definizione di cui alla normativa vigente [3]; per dato personale si intende 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 del SSASP, ovvero chiave pubblica, certificato (se richiesto dal Soggetto), date di revoca e di sospensione del certificato, non sono considerati dati personali.

9.4.4 Titolare del trattamento dei dati personali

Denominazione sociale	**Tinexta Infocert S.p.A**
Sede legale	**Piazzale Flaminio n. 1/B**
	00196 Roma
E-mail	**richieste.privacy@legalmail.it**

9.4.5 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy è disponibile sul sito www.infocert.it. InfoCert procede, se necessario, a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge [3] prima dell'erogazione del servizio. Informative specifiche possono essere presenti sul sito del Cliente, che, qualora necessario, potrebbe raccogliere il consenso al trattamento per conto di InfoCert.

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

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

9.4.7 Altri motivi di divulgazione

Non previsti.

9.5 Proprietà intellettuale

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

9.6 Rappresentanza e garanzie

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

9.7 Limitazioni di garanzia

Infocert non presta alcuna garanzia (i) sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal Soggetto; (ii) su usi della chiave privata, - , 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, della firma qualificata- o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito, ferma restando l'efficacia di firma autografa riconosciuta alla firma elettronica qualificata, ai sensi dell'art. 25 del Regolamento [1]; (v) sulla segretezza e/o integrità

di qualsiasi messaggio, atto o documento associato al certificato di sottoscrizione o confezionato tramite le chiavi a cui il certificato è riferito (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili dal Soggetto o dal destinatario attraverso l'apposita procedura di verifica).

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

9.8 Limitazioni di responsabilità

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

Fatto salvo il caso di dolo o colpa, InfoCert non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo servizio rilasciati in base alle previsioni del presente Manuale

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 Soggetto.

InfoCert, inoltre, fin dalla fase di formazione del Contratto per i servizi di firma remota, 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 Soggetto, 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

Infocert è unicamente responsabile degli eventuali danni direttamente determinati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica, in seguito a un mancato adempimento degli obblighi di cui al Regolamento [1] 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 Soggetto avranno diritto di ottenere, a titolo di risarcimento dei danni direttamente subiti in conseguenza del comportamento di cui al paragrafo precedente, un importo che non potrà in ogni caso essere superiore ai valori massimi previsti, per ciascun sinistro e per anno, dall'art. 3, c. 7, del Regolamento allegato alla Determinazione 185/2017.

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo

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

9.10 Termine e risoluzione

9.10.1 Termine

Prima della scadenza, il Soggetto può richiedere il rinnovo del certificato sia mantenendo le stesse chiavi, sia ri-certificando nuove chiavi, secondo la procedura indicata dal presente Manuale Operativo.

9.10.2 Risoluzione

Il Contratto si risolverà di diritto con contestuale interruzione del Servizio e revoca del certificato emesso nelle ipotesi di mancato adempimento delle clausole tempo per tempo segnalate nel contratto di fornitura del servizio. La risoluzione si verificherà di diritto quando la parte interessata dichiari all'altra a mezzo PEC o lettera raccomandata a.r., che intende avvalersi della presente clausola.

In tutti i casi di risoluzione saranno salvi gli effetti prodotti dal Contratto fino a tale momento.

Il Soggetto prende atto che, in caso di risoluzione del Contratto, per qualsiasi causa essa avvenga, non sarà più possibile usufruire del Servizio.

9.10.3 Effetti della risoluzione

La risoluzione comporta l'immediata disattivazione del servizio.

9.10.4 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1.

9.10.5 Revisione del Manuale Operativo

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

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come, ad esempio, modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo Manuale Operativo verrà prontamente comunicata alle RA e al CAB accreditato.

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

9.10.6 Storia delle revisioni

Informazione	*Dettaglio*
Versione/Release n°:	**1.0**
Data Versione/Release:	**16/03/2026**
Descrizione modifiche:	**Prima versione**
Motivazioni:	**Nuovo Servizio Qualificato**

Tabella 7 – Versione 1.0

9.10.7 Procedure di revisione

La revisione del Manuale Operativo segue le medesime procedure previste per la sua redazione e approvazione, di cui al capitolo 2 del presente documento, nell'ambito del Sistema di Gestione per la Qualità e del Sistema di Gestione per la Sicurezza delle Informazioni adottati da Infocert.

Ogni modifica è sottoposta a verifica interna da parte delle funzioni competenti in materia di sicurezza, compliance, aspetti legali e regolamentari, nonché delle funzioni responsabili dell'erogazione del servizio di firma remota.

Le revisioni sono approvate dalla Direzione Aziendale prima della pubblicazione della nuova versione del documento.

9.10.8 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

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

9.10.9 Casi nei quali l'OID deve cambiare

n/a

9.11 Risoluzione delle controversie

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

9.12 Foro competente

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

9.13 Legge applicabile

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

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

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

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

[3] Decreto 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).

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

[5] Verifica preliminare - 24 settembre 2015 [4367555] Trattamento di dati personali nell'ambito del "Processo di rilascio con riconoscimento a mezzo webcam" per firma elettronica qualificata o digitale.

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

[7] 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.

[8] Certificate Policy - Certificate Practice Statement ICERT-INDI-MO

[9] CPS Addendum – Documenti di identità accettabili.

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

9.14 Disposizioni varie

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

9.15 Altre disposizioni

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

Servizio	*Orario*
Servizio di Firma Remota	**Dalle 0:00 alle 24:00** **7 giorni su 7 (disponibilità minima 99.0%)**

Tabella 26 – orari di erogazione del servizio

APPENDICE A

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

Infocert mette a disposizione un prodotto (denominato "Infocert Sign") gratuitamente scaricabile dai dai Firmatari o dagli Utenti dal sito www.firma.infocert.it per consentire:

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

Gli ambienti in cui Infocert Sign opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo web sopra indicato. Le istruzioni per l'utilizzo del prodotto sono incluse nel prodotto stesso e consultabili tramite la funzione di help. Il prodotto Infocert Sign è in grado di firmare qualsiasi tipo di file. La possibilità di visualizzare il file dipende dalla disponibilità sulla stazione di lavoro dell'utente di un adeguato software di visualizzazione.

Infocert può mettere a disposizione, a pagamento e secondo gli accordi commerciali tempo per tempo stabiliti con le RA, i Richiedenti, i Soggetti o gli Utenti, ulteriori prodotti o servizi di firma e/o di verifica della firma. I documenti elettronici sottoscritti con certificati emessi da Infocert possono essere verificati anche attraverso altri strumenti, in grado di interpretare i formati di firma previsti. Tali strumenti sono fuori dalla responsabilità di Infocert.

Ad esempio, i documenti firmati utilizzando i certificati emessi in virtù del Manuale Operativo della CA Infocert, in formato PAdES, sono verificabili anche con lo strumento Adobe Reader®.

AVVERTENZA

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