Infocert: Manuale Operativo del Servizio di Verifica dell'Identità

Codice documento	ICERT-INDI-IPSPS
Versione	1.2
Data	25/02/2026

tinexta infocert

1 PREMESSA

1.1 Panoramica

Tinexta Infocert (di seguito “Infocert”) è un fornitore di servizi fiduciari che offre anche servizi online per la verifica dell'identità delle persone fisiche a supporto dell'emissione di certificati.

Attraverso i servizi di verifica dell'identità e di certificati qualificati, i singoli clienti possono utilizzare le firme elettroniche in modo legale, secondo il regolamento n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (di seguito "eIDAS" o "Regolamento eIDAS"), nonché, per quanto riguarda il contesto svizzero, alla Legge federale del 18 marzo 2016 sulla firma elettronica e alla relativa Ordinanza del 23 novembre 2016.

In particolare, la soluzione SelfQ verifica l'identità delle persone fisiche in conformità con eIDAS, articolo 24, comma 1, lettera d), utilizzando "altri metodi di identificazione" riconosciuti dalla normativa nazionale che forniscono garanzie equivalenti in termini di affidabilità alla presenza fisica. La conformità ai requisiti eIDAS è verificata dall’Organismo di Valutazione della Conformità CSQA Certificazioni S.r.l., secondo lo standard ETSI EN 119 461 e lo schema di valutazione eIDAS definito da ACCREDIA, in conformità agli standard ETSI EN 319 403 e UNI CEI EN ISO/IEC 17065:2012.

Il presente documento rappresenta il *Trust Service Practice Statement* della soluzione SelfQ. Non si tratta di una Certification Practice Statement (CPS) completa ai sensi della RFC 3647, poiché riguarda esclusivamente l’erogazione dei servizi di verifica dell’identità e non include altri servizi di certificazione, quali l’emissione o la validazione dei certificati (si veda ICERT-INDI-MO per i servizi di certificazione Infocert [10]).

Lo scopo di questo documento è quello di fungere da base per la conformità con eIDAS e ZertES.

1.2 Nome e identificazione del documento

Il presente documento, intitolato **“Infocert: Manuale Operativo del servizio di verifica dell’identità”** (codice documento: ICERT-INDI-IPSPS), descrive le politiche e le procedure adottate per la gestione del Servizio di Identity Proofing di Infocert in conformità al Regolamento eIDAS [1].

Questo documento è associato a uno o più Object Identifier (OID) descritti di seguito.
L'*Object Identifier* (OID) che identifica Infocert è 1.3.76.36.

Di seguito sono elencate le politiche per il metodo di identificazione:

Descrizione	*OID*
Casi d'uso che prevedono l'utilizzo di un documento d'identità per la verifica remota non presidiata dell’identità, con funzionamento ibrido manuale e automatizzato: SelfQ	1.3.76.36.1.1.5000.34

(Conforme ai requisiti della norma ETSI TS 119 461 stabiliti nel capitolo 9.2.3.3 "Caso d'uso per il funzionamento ibrido manuale e automatico").	
Casi d'uso che prevedono l'utilizzo di un documento d'identità per la verifica remota non presidiata dell'identità, con funzionamento ibrido manuale e automatizzato: SelfQ automatizzato *(Conforme ai requisiti di ETSI TS 119 461 stabiliti nel capitolo 9.2.3.4 "Caso d'uso per il funzionamento automatizzato")*	1.3.76.36.1.1.5000.34

Tabella 1 - Politiche per il metodo di verifica dell'identità

1.3 Partecipanti IPSP

IPSP: Identity Proofing Service Provider

I dettagli completi dell'organizzazione che funge da IPSP sono i seguenti:

Nome della società	**Tinexta Infocert SpA - Società per azioni Società soggetta alla direzione e al coordinamento di Tinexta S.p.A.**
Sede legale	**Piazzale Flaminio n.1/B, 00196, Roma, Italia**
Uffici operativi	**Via Fernanda Wittgens n. 2, 20123 Milano (MI)** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Rappresentante legale	**Danilo Cattaneo - Amministratore Delegato**
Numero REA	**RM - 1064345**
Numero di partita IVA	**07945211006**
Sito web	**https://www.infocert.it**

TSP/QTSP: il fornitore di servizi che gestisce il processo ed emette i certificati. Potrebbe essere InfoCert che agisce come QTSP.

Richiedente o Soggetto: l'individuo sottoposto a identificazione.

Operatore di back-office: una persona adeguatamente formata che segue le istruzioni fornite dall'IPSP e verifica i risultati della validazione.

1.4 Amministrazione politica e pratica

1.4.1 Contatti

InfoCert è responsabile della definizione, dell'aggiornamento e della pubblicazione del presente documento.

Per domande, reclami, commenti e richieste di chiarimento in merito al presente Manuale Operativo, si prega di contattare:

Nome della società	**InfoCert – S.p.A** **Responsabile QTSP** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Numero di telefono	**+39 06 836691**
Firma digitale Contact Center	**https://help.infocert.it/contatti/ per maggiori dettagli**
Sito web	**https://www.firma.infocert.it,https://www.infocert.it**
E-mail	**firma.digitale@legalmail.it**

I soggetti possono richiedere una copia della propria documentazione personale compilando e inviando il modulo disponibile sul sito https://www.firma.infocert.it, seguendo la procedura indicata.

1.4.2 Soggetti responsabili dell'approvazione del presente documento

Il presente Manuale Operativo del servizio di Verifica dell'Identità (di seguito IPSPS) è stato approvato dalla Direzione aziendale a seguito di una revisione da parte del Responsabile della sicurezza e delle politiche, del Responsabile della privacy, del Responsabile dei servizi di certificazione, del Responsabile dell'ufficio legale e del Responsabile degli affari normativi.

1.4.3 Procedure di approvazione

La redazione e l'approvazione del presente documento avvengono in conformità alle procedure descritte nel Sistema di gestione della qualità aziendale ISO 9001:2015.

Almeno una volta all'anno, InfoCert verifica la conformità di questa Dichiarazione di prassi sul Verifica dell'identità con il suo processo di servizio di certificazione.

1.5 Definizioni e acronimi

1.5.1 Definizioni

Termine	*Definizione*
Sigillo elettronico avanzato	Sigillo elettronico che soddisfa i requisiti di cui all'articolo 36 del Regolamento eIDAS (cfr. eIDAS [1]) e all'art. 2 della normativa ZertES.
Firma elettronica avanzata	Firma elettronica che soddisfa i requisiti di cui all'articolo 26 del Regolamento eIDAS (cfr. eIDAS [1]) e all'art. 2 della normativa ZertES.
Richiedente (applicant)	Persona (fisica o giuridica) la cui identità deve essere verificata [6].
Registro di controllo (audit log)	Insieme delle registrazioni, automatiche o manuali, degli eventi previsti dai Requisiti Tecnici.
Associazione al richiedente (binding to applicant)	Parte del processo di identificazione che verifica che il richiedente sia effettivamente la persona identificata sulla base delle evidenze presentate [6].

Organismo di valutazione della conformità - *Conformity Assessment Body (CAB)*	**Organismo di Valutazione della Conformità (CAB)** Organismo accreditato ai sensi del Regolamento eIDAS o della normativa ZertES, competente a valutare la conformità di un prestatore qualificato di servizi fiduciari e dei relativi servizi fiduciari qualificati. È responsabile della redazione del CAR.
Conformity Assessment Report (CAR) - *Rapporto di valutazione della conformità*	Relazione con cui l'Organismo di Valutazione della Conformità attesta che il prestatore qualificato di servizi fiduciari e i servizi da esso forniti sono conformi ai requisiti del Regolamento eIDAS (cfr. eIDAS [1]).
Cliente (customer)	Soggetto con il quale InfoCert ha formalizzato un contratto di fornitura di servizi a fronte di un corrispettivo.
Documento di identità digitale	Documento di identità rilasciato in formato validabile automaticamente, firmato digitalmente dall'emittente e disponibile esclusivamente in forma digitale [6]
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazioni sonore, visive o audiovisive (cfr. eIDAS [1]).
Mezzi di identificazione elettronica	Unità materiale e/o immateriale contenente dati di identificazione personale, utilizzata per accedere a servizi online (vedi eIDAS [1]).
Identificazione elettronica	Processo di utilizzo di dati di identificazione personale in formato elettronico che rappresentano in modo univoco una persona fisica o giuridica, oppure una persona fisica che rappresenta una persona giuridica (vedi eIDAS [1]).
Identità	Attributo o insieme di attributi che identificano in modo univoco una persona in un determinato contesto [6].
Documento d'identità	Documento fisico o digitale rilasciato da un'autorità competente che attesta l'identità del richiedente [6].
Verifica dell'identità (identity proofing)	Processo mediante il quale l'identità di un richiedente viene verificata attraverso evidenze attestanti gli attributi di identità richiesti [6].
Fornitore di Servizi di Verifica dell'identità (Identity Proofing Service Provider)	Entità specializzata che fornisce servizi di identificazione in qualità di subfornitore di un prestatore di servizi fiduciari (TSP), erogando una componente del servizio fiduciario del TSP.
liveness detection	Misurazione e analisi di caratteristiche anatomiche o di reazioni involontarie o volontarie, finalizzate a determinare se un campione biometrico sia acquisito da un soggetto vivo presente al momento della rilevazione [6].
Dati di identificazione personale	Insieme di dati utilizzati per determinare l'identità di una persona fisica e/o giuridica o di una persona fisica che rappresenta una persona giuridica (cfr. eIDAS [1]
Presenza fisica	Modalità di identificazione che richiede la presenza fisica del richiedente nel luogo in cui si svolge il processo di identificazione [6].
Attacco di presentazione	Presentazione al sottosistema di acquisizione dei dati biometrici con l'obiettivo di interferire con il funzionamento del sistema biometrico [5].
Rilevamento degli attacchi di presentazione	Determinazione automatica di un attacco di presentazione [6].
Firma elettronica qualificata	Firma elettronica avanzata creata mediante un dispositivo qualificato per la creazione di firme elettroniche e basata su un certificato qualificato di firma elettronica (vedere eIDAS [1]
Certificato di firma elettronica qualificata	Certificato di firma elettronica emesso da un prestatore di servizi fiduciari qualificato e conforme ai requisiti dell'allegato I del Regolamento eIDAS (cfr. eIDAS [1]) o della normativa ZertES.
Servizio fiduciario qualificato	Servizio fiduciario che soddisfa i requisiti applicabili stabiliti dal Regolamento eIDAS ([1]).
Qualified Trust Service Provider - Fornitore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari che fornisce uno o più servizi fiduciari qualificati. Il suo status qualificato è concesso dall'organismo di vigilanza (cfr. eIDAS [1]).

Richiedente	Una persona fisica o giuridica che si affida a un servizio di identificazione elettronica o a un servizio fiduciario (cfr. eIDAS [1]).
Soggetto	Persona fisica o giuridica iscritta ad un servizio fiduciario [6].
Firmatario	Persona fisica o giuridica vincolata da un accordo con un prestatore di servizi fiduciari in relazione agli obblighi del sottoscrittore [6].
Servizio fiduciario	Servizio elettronico normalmente fornito a fronte di un corrispettivo che consiste in: a) creazione, verifica e validazione di firme elettroniche, sigilli elettronici o marche temporali elettroniche, servizi elettronici di recapito certificato e relativi certificati; oppure b) creazione, verifica e validazione di certificati per l'autenticazione di siti web; oppure c) conservazione di firme elettroniche, sigilli elettronici o certificati relativi a tali servizi (cfr. eIDAS [1]).
Manuale Operativo del servizio fiduciario - Trust Service Practice Statement	Documento descrittivo delle policy relative al TSP che fornisce un servizio fiduciario [3].
Trust Service Provider - Fornitore di servizi fiduciari	Persona fisica o giuridica che fornisce uno o più servizi fiduciari in qualità di prestatore qualificato o non qualificato (vedi eIDAS [1]).
Verifica dell'identità remota non assistita	Processo di identificazione effettuato da remoto mediante utilizzo di un documento di identità, in cui l'acquisizione del documento (fisico o digitale) e del video del volto del richiedente avvengono in una sessione automatizzata e interattiva, senza supervisione umana [6].
VIZ	La zona di ispezione visiva (Visual Inspection Zone) del documento ID è costituita da una serie di zone di testo che contengono un insieme predeterminato di informazioni di base.

1.5.2 Acronimi

Acronimo	*Significato*
AgID	Agenzia per l'Italia Digitale: Autorità di vigilanza per i prestatori di servizi fiduciari
CAB	Conformity Assessment Body - Organismo di valutazione della conformità
CAR	Conformity Assessment Report - Rapporto di valutazione della conformità
DNN	Deep Neural Network - Rete neurale profonda
eMRTD	Electronic Machine-Readable Travel Document - Documento di viaggio elettronico a lettura ottica
EIC	Electronic Identity Card - Carta d'identità elettronica
eIDAS	Electronic Identification, Authentication and Trust Services - Identificazione elettronica, autenticazione e servizi fiduciari [1]
eID	Electronic Identity - Identità elettronica
ETSI	European Telecommunications Standards Institute - Istituto europeo per gli standard di telecomunicazione
GDPR	General Data Protection Regulation - Regolamento generale sulla protezione dei dati [2]
ISO	International Organization for Standardization - Organizzazione internazionale per la standardizzazione: Fondata nel 1946, l'ISO è un'organizzazione internazionale composta da organismi nazionali di standardizzazione

IPSP	Identity Proofing Service Provider - Fornitore di Servizi di Verifica dell'identità
IPSPS	Identity Proofing Service Practice Statement – Manuale operativo del servizio di verifica dell'identità
LoA	Level of Assurance - Livello di garanzia
MRZ	Machine Readable Zone - Zona leggibile dalla macchina
OCR	Optical Character Recognition - Riconoscimento ottico dei caratteri
OID	Object Identifier: una sequenza di numeri registrata secondo la procedura indicata nella norma ISO/IEC 6523, che fa riferimento a un oggetto specifico all'interno di una gerarchia
PAD	Presentation Attack Detection - Rilevamento degli attacchi di presentazione
PEC	Posta Elettronica Certificata (Certified e-mail)
QTSP	Qualified Trust Service Provider - Fornitore di servizi fiduciari qualificato
TSP	Trust Service Provider - Fornitore di servizi fiduciari
VIZ	Visual Inspection Zone - Zona di ispezione visiva
VZertES	Ordinanza svizzera sui servizi di certificazione relativi alle firme elettroniche e ad altre applicazioni dei certificati digitali, che integra la Legge federale ZertES.
ZertES	Legge federale svizzera che disciplina le condizioni alle quali i fornitori di servizi fiduciari possono utilizzare servizi di certificazione con firme elettroniche.

1.6 Riferimenti

1. Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, versione consolidata: 18/10/2024, come modificato dal Regolamento (UE) n. 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 (di seguito denominato eIDAS).

2. GDPR (General Data Protection Regulation) Regolamento UE 679/2016 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.

3. ETSI EN 319 401: "Firme elettroniche e infrastrutture fiduciarie (ESI); requisiti di politica generale per i fornitori di servizi fiduciari".

4. ETSI EN 319 411-1: "Firme elettroniche e infrastrutture (ESI); requisiti di politica e di sicurezza per i prestatori di servizi fiduciari che rilasciano certificati; Parte 1: Requisiti generali".

5. ETSI EN 319 411-2: "Firme elettroniche e infrastrutture (ESI); requisiti di politica e di sicurezza per i prestatori di servizi fiduciari che rilasciano certificati; Parte 2: Requisiti per i prestatori di servizi fiduciari che emettono certificati qualificati UE".

6. ETSI TS 119 461: "Firme elettroniche e infrastrutture fiduciarie (ESI); requisiti di politica e sicurezza per i componenti dei servizi fiduciari che forniscono la verifica dell'identità dei soggetti dei servizi fiduciari".

7. ICAO Doc 9303 parte 3: Documenti di viaggio a lettura ottica Ottava edizione, 2021 Parte 3: Specifiche comuni a tutti gli MRTD.

8. ICAO Doc 9303 parte 4: Documenti di viaggio a lettura ottica Ottava edizione, 2021 Parte 4: Specifiche per i passaporti a lettura ottica (MRP) e altri MRTD in formato TD3.

9. ICAO Doc 9303 parte 10: "Documento di viaggio a lettura ottica - Parte 10: Struttura logica dei dati (LDS - Logical Data Structure) per la memorizzazione di dati biometrici e altri dati nel circuito integrato (IC) senza contatto".

10. Politica di certificazione & Dichiarazione di pratica di certificazione InfoCert: ICERT-INDI-MO.

11. Manuale di conservazione InfoCert: 01_Preservation_Manual_of_InfoCert_ENG_2023
12. ZertES (RS 943.03), Legge federale sulle firme elettroniche del 18 marzo 2016 in Svizzera e successive modifiche.
13. VZertES (RS 943.032), Ordinanza sulla legge sulla firma elettronica e successive modifiche.

14. TAV (RS 943.032.1), Servizi di certificazione nell'ambito della firma elettronica e altre applicazioni dei certificati digitali.

2 PROCESSO DI VERIFICA DELL'IDENTITÀ

2.1 Fasi del processo SelfQ

Il Richiedente è guidato attraverso un processo end-to-end che fornisce un'esperienza di identificazione non presidiata, composta dalle seguenti fasi:

Raccolta dati:

Il Richiedente riceve una guida automatica durante l'intero processo di verifica dell'identità, comprese le condizioni necessarie al suo completamento con successo.

Si noti che solo i documenti di identità digitale eMRT conformi alla norma ICAO 9303 parte 10 [9] sono accettati.

- Il Richiedente acquisisce le immagini del proprio documento d'identità tramite un'applicazione mobile guidata o un'interfaccia web (non è consentito il caricamento).
- Il servizio SelfQ OCR estrae i dati dal documento d'identità, consentendo al richiedente di confermare o correggere piccoli errori.

I documenti d'identità variano a seconda delle regioni geografiche, delle versioni e del loro utilizzo.

Il prestatore di servizi fiduciari può limitare i documenti accettabili. Quando si applica la legge ZertES, i documenti di identità accettati sono: la carta d'identità svizzera, le carte d'identità dei Paesi dell'area Schengen oppure il passaporto.

I documenti di identità contengono generalmente informazioni sia sul fronte sia sul retro (vi sono pochi casi in cui le informazioni sono presenti solo sul fronte). Le informazioni contenute nel documento di identità possono essere suddivise in due categorie: VIZ e MRZ.

La VIZ **(Visual Inspection Zone)**, dove appaiono le informazioni sul proprietario del documento d'identità, contiene i seguenti elementi:

- Viso: Fotografia del volto della persona identificata dal documento.
- Nodi OCR: Contengono le informazioni scritte del documento, come nomi, cognomi, date, numero di identificazione, numero di supporto, indirizzi, ecc.
- Caratteristiche di sicurezza fisica: Misure di sicurezza fisica come inchiostri OVI, microscrittura, Kinegrams, ecc.

La MRZ **(Machine Readable Zone**) è l'area del documento d'identità in cui compaiono le informazioni adatte a essere lette da una macchina. In genere è composto da due righe (passaporto) o da tre righe (carta d'identità). Vedi [7] e [8].

Le categorie di dati estratti dai documenti d'identità possono essere diverse a seconda del tipo di documento e del suo modello di riferimento. I dati comuni estratti possono essere ripresi come segue:

- **Nome**
- **Cognome**
- **Sesso**
- **Codice fiscale**
- Data di nascita
- Luogo di nascita
- Nazionalità
- Indirizzo relativo al luogo di residenza
- Numero del documento
- Paese di emissione
- Valido da (data)
- Valido fino a (data)
- Luogo di emissione

Convalida dei dati:

- Il sistema verifica se il documento d'identità è stato manomesso, la coerenza di MRZ e VIZ e gli indicatori antifrode (basati su controlli di replay e attacchi di stampa).
- Le informazioni della MRZ vengono estratte, convalidate e confrontate con quelle della parte visibile del documento d'identità.

Vincolante per il Richiedente:

- Il Richiedente esegue una breve sessione video per il rilevamento della vitalità (*liveness detection*). Durante la sessione video, eseguita esclusivamente al momento del processo di verifica dell'identità, viene effettuata una ripresa video. Quando tutte le caratteristiche qualitative corrispondono (illuminazione, posizione, risoluzione), il sistema prende automaticamente le immagini del richiedente dal video e il software le elabora in tempo reale, determinando il corretto allineamento del volto.
- Una volta estratta l'immagine del volto del richiedente, il sistema la confronta con l'immagine estratta dal documento d'identità precedentemente raccolto.

La fase di *liveness detection* risponde alla necessità di verificare la presenza e l'effettiva esistenza dell'utente, che sottopone a verifica il proprio volto rispetto alla foto estratta dal proprio documento d'identità. Il servizio permette di:

- Guidare l'utente nel processo di inquadratura del viso per scattare un selfie che

garantisca le condizioni ottimali:
    - Allineamento del volto durante l'istantanea.
    - Qualità dell'immagine acquisita.
    - Luce dell'immagine catturata.
- Eseguire il riconoscimento del volto "in diretta" durante la procedura.

Il modulo di *liveness detection* assicura che davanti alla telecamera si trovi una persona reale, non una foto o un video in streaming. InfoCert guida l'intero processo di raccolta dei dati e crea un breve video in cui i pixel vengono analizzati ed elaborati automaticamente per prevenire i tentativi di frode. Tutta la tecnologia si basa su componenti AI altamente sofisticati, che consistono in reti neurali opportunamente addestrate, con una serie di coefficienti che minimizzano l'errore e sono in grado di classificare i dati in entrata, successivamente utilizzati per attività vincolanti.

In particolare, il modulo è in grado di identificare i tentativi di spoofing basati sullo stesso selfie utilizzato per la corrispondenza del volto, senza la partecipazione dell'utente, e impiega un metodo basato sulla cosiddetta Deep Neural Network (DNN), che esamina vari elementi dell'immagine per rilevare gli artefatti che aiutano a distinguere tra la foto di una persona in carne e ossa e un cosiddetto "attacco di presentazione" (*presentation attack*).

Il componente di rilevamento della *liveness detection* di Infocert è stato valutato in conformità allo standard ISO/IEC 30107-3:2023, relativo a "*Information technology - Biometric presentation attack detection*", ottenendo il livello "substantial" (significativo). Sono state eseguite valutazioni e test per attacchi di tipo 1 (attacchi di presentazione) e di tipo 2 (attacchi di iniezione).

Inoltre, il componente di rilevamento della *liveness detection* è conforme alle caratteristiche specificate nell'obiettivo di sicurezza per il livello di valutazione "significativo", come definito nella norma CEN TS 18099 e nel piano di test CLR Labs associato al livello significativo di certificazione. Sono stati eseguiti test sulle funzioni di rilevamento degli attacchi di iniezione.

Il flusso video viene trasmesso a un ambiente che garantisce l'autenticità, l'integrità e la riservatezza dell'elemento prodotto.

Una volta terminato il rilevamento *liveness detection*, il componente automatico di corrispondenza dei volti confronta il volto dell'utente mostrato nel selfie con la foto estratta dal documento d'identità.

La revisione opzionale degli operatori di back-office garantisce un'ulteriore precisione.

Rilascio del risultato della verifica dell'identità:

Una volta che tutti i controlli sono stati eseguiti dal sistema con esito positivo, è possibile rilasciare un certificato qualificato.

I dati e le prove sono conservati digitalmente dal QTSP per il periodo previsto dalle norme e dai regolamenti locali. Se il QTSP è InfoCert, tali dati e prove sono conservati digitalmente per 20 (venti) anni.

3 CONTROLLI DI STRUTTURA, DI GESTIONE E OPERATIVI

InfoCert ha implementato un sistema di sicurezza informatica per i suoi servizi di fiducia. Il sistema di sicurezza è suddiviso in tre livelli:

- Un livello fisico volto a garantire la sicurezza degli ambienti in cui il TSP gestisce il servizio.
- Un livello procedurale di natura strettamente organizzativa.
- Un livello logico che prevede la fornitura di tecnologie hardware e software per affrontare i problemi e i rischi associati al tipo di servizio e all'infrastruttura utilizzata.

Questo sistema di sicurezza è progettato per evitare i rischi derivanti dal malfunzionamento di sistemi, reti e applicazioni, nonché dall'intercettazione o dalla modifica non autorizzata dei dati.

Un estratto della politica di sicurezza Infocert può essere richiesto via e-mail a *infocert@legalmail.it.*

Le politiche di sicurezza Infocert vengono riviste almeno una volta all'anno e aggiornate in base a eventuali modifiche. Ogni revisione viene tracciata all'interno del documento stesso, anche quando non sono necessarie modifiche.

I controlli di sicurezza fisica, la gestione del sito, l'accesso fisico, la prevenzione e la protezione contro inondazioni e incendi, la gestione della conservazione e altri controlli operativi sulla struttura e sulla sicurezza sono gestiti da Infocert in qualità di QTSP e descritti in ICERT-INDI-MO [10].

3.1 Controlli procedurali del personale

3.1.1 Ruoli chiave

I ruoli chiave sono ricoperti da personale in possesso delle necessarie esperienze, professionalità e competenze tecnico-giuridiche, costantemente verificate attraverso valutazioni annuali.

3.1.2 Qualifiche, esperienza e requisiti di autorizzazione

A seguito della pianificazione annuale delle risorse umane, il Responsabile di funzione/struttura organizzativa individua le caratteristiche e le competenze della risorsa da inserire (job profile). Successivamente, in collaborazione con il Responsabile della selezione del personale, vengono avviati il processo di ricerca e selezione. I candidati selezionati partecipano al processo di selezione sostenendo un primo colloquio conoscitivo-motivazionale con il Responsabile della selezione del personale e un successivo colloquio tecnico con il Responsabile della funzione/struttura organizzativa, al fine di verificare le competenze dichiarate dal candidato. Ulteriori strumenti di verifica sono le esercitazioni e i test.

3.1.3 Requisiti per la formazione

Per evitare che qualcuno possa influenzare o alterare individualmente la sicurezza complessiva del sistema o svolgere attività non autorizzate, la gestione operativa del sistema è affidata a diverse risorse, ciascuna con compiti distinti e ben definiti. Il personale incaricato della progettazione del servizio di Identity proofing è stato selezionato per il suo background nella progettazione, implementazione e gestione di servizi IT e per le sue caratteristiche di affidabilità e riservatezza. Periodicamente sono previste sessioni di formazione per sensibilizzare il personale sui compiti assegnati. In particolare, prima dell'inserimento del personale nelle attività operative, vengono effettuati corsi di formazione per fornire tutte le competenze (tecniche, organizzative e procedurali) necessarie a svolgere i compiti assegnati.

3.1.4 Frequenza di riqualificazione

Ogni inizio d'anno vengono analizzati i fabbisogni formativi per definire i corsi di formazione da tenere nel corso dell'anno. L'analisi si basa sulle seguenti fasi:

- Incontro con la direzione aziendale per raccogliere dati sui requisiti di formazione necessari per raggiungere gli obiettivi aziendali.
- Feedback dei responsabili di area per identificare le esigenze formative specifiche di ciascuna area.
- Inoltro dei dati raccolti alla Direzione aziendale per la chiusura e l'approvazione del Piano di formazione.

Una volta definito, il Piano di formazione viene condiviso con il personale all'inizio dell'anno.

3.1.5 Sanzioni per azioni non autorizzate

Le sanzioni sono comminate al personale dipendente in conformità al Contratto Nazionale di Lavoro dei metalmeccanici e degli installatori di impianti industriali privati ("CCNL Metalmeccanici e installatori industria privata").

3.1.6 Controlli sul personale non dipendente

L'accesso al personale non dipendente è regolato da una specifica politica aziendale. Partecipano a una formazione adeguata.

3.1.7 Documentazione da fornire da parte del personale

Al momento dell'assunzione, i dipendenti devono fornire una copia di un documento d'identità valido, nonché una copia di una tessera sanitaria valida e una foto tipo passaporto per il badge di accesso. Successivamente, dovranno compilare e firmare un consenso scritto al trattamento dei dati personali e un accordo di riservatezza, nonché prendere visione del Codice etico e della Netiquette di Infocert.

4 PROCEDURE DI REGISTRAZIONE DEGLI AUDIT

4.1 Tipi di eventi registrati

Le prove, gli eventi e i registri del processo di verifica dell'identità sono raccolti e conservati in conformità al metodo di verifica dell'identità scelto. In alcuni casi, a seconda del contesto, è possibile raccogliere e conservare anche la prova di convalida.

Le procedure per la gestione delle evidenze, degli eventi e dei log relativi al funzionamento del servizio di identity proofing sono formalizzate in una procedura interna.

Vengono raccolti mediante procedure automatizzate ad hoc.

4.2 Periodo di conservazione

Tutte le prove, i registri e gli eventi vengono conservati per almeno 5 (cinque) anni, anche se la verifica dell'identità è stato rifiutato; al termine del periodo di conservazione definito, le prove del processo di verifica dell'identità e tutti i dati personali del richiedente saranno cancellati.
Il fornitore di identity proofing può conservare le prove e i registri per un periodo di tempo più lungo, in base ad accordi specifici con il TSP che utilizza il servizio.

4.3 Come vengono conservate le prove

Le prove del processo di verifica dell'identità vengono conservate in modo antimanomissione, garantendo la riservatezza delle informazioni.

L'obiettivo è garantire la possibilità di cercare, recuperare e verificare nuovamente i risultati della verifica dell'identità per mantenerli facilmente accessibili su richiesta delle forze dell'ordine o dell'interessato.

Le prove sono conservate nel sistema di archiviazione Infocert SAFE LTA (cfr. 01_Preservation_Manual_of_InfoCert_ENG_2023) [11].

5 ALTRE QUESTIONI COMMERCIALI E LEGALI

5.1 Corrispettivi

Le tariffe per i servizi di verifica dell'identità sono soggette ad accordi contrattuali tra Infocert e i suoi partner commerciali.

5.2 Responsabilità finanziaria

5.2.1 Copertura assicurativa

Infocert dispone di una copertura assicurativa per la responsabilità professionale.

5.3 Privacy Informazioni personali

Se non espressamente consentito, tutte le informazioni acquisite dall'IPSP nel corso delle sue attività di routine sono riservate e non divulgabili, ad eccezione delle informazioni specificamente destinate all'uso pubblico. I dati personali saranno trattati dall'IPSP nel rispetto del Decreto Legislativo 30 giugno 2003, n. 196 e del Regolamento Europeo 2016/679 (GDPR) in vigore dal 25 maggio 2018 [2].

5.3.1 Piano per la privacy

Infocert implementa le politiche di protezione dei dati personali all'interno del proprio sistema di gestione della sicurezza delle informazioni certificato ISO 27001, garantendo un miglioramento continuo.

5.3.2 Informazioni personali

Dati personali così come definiti dalla normativa vigente [2] si riferiscono a qualsiasi informazione su una persona **fisica** che possa identificarla, direttamente o indirettamente, compreso un numero di identificazione personale.

I dipendenti di Infocert che gestiscono le informazioni sono tenuti a proteggere tali dati dalla compromissione e dalla divulgazione a terzi.

Sono tenuti a rispettare le leggi italiane sulla privacy.

5.3.3 Titolare del trattamento dei dati personali

Nome della società	**Tinexta Infocert SpA**
Sede legale	**Piazzale Flaminio n. 1/B** **00196 Roma**
E-mail	**richieste.privacy@legalmail.it**

5.3.4 Informativa sulla privacy e consenso

L'informativa sulla privacy di Infocert è disponibile sul sito web www.infocert.it al seguente link:

https://www.infocert.it/informative-privacy.

Infocert tratterà i dati nei modi e nelle forme previste dalla legge. Il trattamento sarà basato su una base giuridica appropriata, come descritto nell'informativa sulla privacy.

Nei casi in cui l'identificazione richieda il trattamento di dati biometrici, Infocert richiederà il consenso prima di fornire il servizio.

Se il trattamento è effettuato da un'altra entità giuridica per conto di Infocert, l'informativa sulla privacy sarà resa disponibile dalla terza parte, che sarà anche responsabile, se necessario, dell'ottenimento del consenso.

5.3.5 Divulgazione conseguenti a richieste legali

Infocert deve divulgare le informazioni richieste dalle autorità, seguendo le procedure stabilite dall'Autorità competente.

5.4 Diritti di proprietà intellettuale

5.5 Dichiarazioni e garanzie

Infocert rimane responsabile del rispetto della propria politica di sicurezza delle informazioni, anche quando alcune funzioni vengono esternalizzate a terzi.

Il Soggetto è responsabile dell'accuratezza dei dati forniti. Se il Soggetto nasconde la propria identità o dichiara falsamente di essere un'altra persona attraverso metodi quali la falsificazione o l'alterazione di documenti, è responsabile di eventuali danni causati all'IPSP e/o a terzi e deve ritenere esonerato l'IPSP da eventuali richieste di risarcimento.

5.6 Esclusione di garanzia

Non viene fornita alcuna garanzia.

5.7 Limitazione di responsabilità

Infocert non è responsabile del controllo del contenuto, del tipo o del formato dei documenti trasmessi dal Soggetto, né di garantire la validità e la tracciabilità della procedura che riflette l'effettivo intento del Soggetto.

Salvo il caso di dolo o colpa grave, Infocert non è responsabile di alcun danno diretto o indiretto ai Soggetti e/o a terzi a causa dell'uso o del mancato uso dei certificati di sottoscrizione emessi dopo il processo di verifica dell'identità.

Infocert declina inoltre ogni responsabilità per eventuali danni diretti e/o indiretti derivanti da: (i) perdita, (ii) conservazione impropria, (iii) uso improprio degli strumenti di identificazione e autenticazione e/o (iv) mancata osservanza da parte del Soggetto delle raccomandazioni di cui sopra.

Inoltre, Infocert non è responsabile di eventuali danni e/o ritardi dovuti a malfunzionamenti del sistema o della rete durante il processo di verifica dell'identità.

Salvo il caso di dolo o colpa grave, Infocert non è responsabile per danni diretti o indiretti al Soggetto.

5.8 Indennità

Infocert è l'unica responsabile per i danni diretti, causati intenzionalmente o per negligenza, a qualsiasi individuo o entità, dovuti alla non conformità con i Regolamenti eIDAS [1] e alla mancata implementazione di misure appropriate per prevenire i danni.

I rimborsi non saranno concessi se i problemi di accesso sono dovuti a un uso improprio del servizio di certificazione, a problemi della rete di telecomunicazione o a eventi al di fuori del controllo di Infocert, come scioperi di forza maggiore, rivolte, terremoti, atti di terrorismo, sommosse popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerre, alluvioni, misure imposte dal governo, hardware e/o software utilizzati dal Richiedente.

5.9 Durata e risoluzione

5.9.1 Termini e Condizioni

Il Richiedente viene informato dei termini e delle condizioni che devono essere accettate prima di iniziare il processo di verifica dell'identità. I termini e le condizioni possono essere applicati all'utilizzo del servizio fiduciario per il quale viene effettuato la verifica dell'identità.

5.9.2 Risoluzione

Il presente CPS rimane in vigore fino a diversa comunicazione da parte di Infocert sul proprio sito web.

5.10 Emendamenti

L'IPSP si riserva il diritto di modificare il presente documento per motivi tecnici o per conformarsi a modifiche legali o normative. Ogni nuova versione sostituisce le precedenti.

L'aumento del numero di release del documento indica modifiche che non hanno un impatto significativo sulle parti interessate, mentre l'aumento del numero di versione del documento indica modifiche che hanno un impatto significativo sulle parti interessate (come, ad esempio, modifiche significative alle procedure operative). In ogni caso, questo documento sarà prontamente pubblicato e reso disponibile nei modi previsti.

Le modifiche importanti richiedono un audit da parte di un CAB accreditato, la presentazione del rapporto di certificazione (CAR - Conformity Assessment Report) e l'approvazione da parte di AgID prima della pubblicazione.

5.10.1 Cronologia degli emendamenti

Informazioni	Descrizione
Versione/Release:	1.2
Versione/data release (gg/mm/aaaa):	25/02/2026
Descrizione modifiche:	§ 1.1, 1.5.1 Integrazione riferimenti normativi (normativa svizzera) § 1.6 Aggiornamento riferimenti normativi § 2.1 Integrazione delle fasi del processo SelfQ § 1.5.2 Aggiornamento della tabella degli acronimi Aggiornamento della denominazione sociale Tinexta Infocert
Motivazioni:	aggiornamenti e integrazioni

Informazioni	Descrizione
Versione/Release:	1.1
Versione/data release (gg/mm/aaaa):	10/07/2025
Descrizione modifiche:	Modifiche alla riformulazione § 5.9 Modifiche alla Risoluzione del servizio
Motivazioni:	aggiornamento del documento

Informazioni	Descrizione
Versione/Release:	1.0
Versione/data release (gg/mm/aaaa):	15/03/2025
Descrizione modifiche:	
Motivazioni:	prima versione

6 ALLEGATO

6.1 Tecnologie in outsourcing

Per alcuni componenti legati ai processi, Infocert si affida alle tecnologie fornite dai seguenti fornitori:

- **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.**
  Disponibile al seguente link: https://veridas.com/en/.
  Veridas è il fornitore di tutti i componenti di raccolta, estrazione e validazione dei dati e delle prove relativi al processo di identificazione SelfQ.
  Per migliorare l'affidabilità del processo di raccolta e convalida delle prove, solo i documenti di identità digitale eMRT conformi alla norma ICAO 9303 parte 10 [9] sono accettati dalla soluzione Veridas.
  Veridas ha ottenuto le certificazioni ETSI TS 119 461 e ETSI EN 319 401, come descritto al seguente link https://veridas.com/en/compliance/

  IDrND
  Disponibile al seguente link: https://www.idrnd.ai/.
  Il modulo Infocert per la *liveness detection* viene messo a disposizione di Infocert dal fornitore ID R&D. I suoi componenti sono conformi e certificati secondo lo standard ISO 30107-3, come indicato nella lettera di conferma di iBeta riportata di seguito (disponibile al seguente link https://www.ibeta.com/wp-content/uploads/2020/10/200930-ID-RD-PAD-Level-2-Confirmation-Letter.pdf).