Identity Proofing Service Practice Statement

Ver. 1.6

10 Novembre 2026

History

ID	Cambiamenti	Rev.	Data	Autore	Verificato	Approvato
IPSPS	Prima versione in italiano.	1.0	15/12/25	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Aggiunti §3.2.4, §3.3.4, §3.4.7, §3.4.8, §3.4.9	1.1	15/04/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Aggiunti §3.1.9 (Identity Proofing con PID EUDIW + eMRTD NFC) e §3.1.10 (Unattended Remote ID Proofing eMRTD); nuovi OID 9.7 e 9.8 nella tabella §1.2; allineamento a EAAS Practice Statement e EAAS Service Policy	1.2	04/06/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Aggiunti §3.2.4.2 Procedura operativa di gestione, §3.4.9.1 Elenco dei registri e delle fonti. Modifica §3.3.4 Modalità di acquisizione dei dati	1.3	26/06/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Revisione generale dei paragrafi §1.2, §3.1, §3.2, §3.3, §3.4, §3.5, §3.6, §4.4.3	1.4	11/08/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Inserimento tabella di risoluzione nel paragrafo 3.3.4 Freshness	1.5	15/10/26	D.Saccò	F.Barcellini	P.Sironi

IPSPS	Revisione paragrafi §1.2, §1.4.3, §3.1, §3.1.3, §3.1.4, §3.1.5, §3.2, §3.2.2, §3.3.1, §3.3.2, §3.3.3, §3.3.4, §3.4.3, §3.4.4, §3.4.6, §3.5.4, §3.5.5, §3.5.6, §3.6.1, §3.6.2, §4.4.3, §4.6.1, §4.6.2, §5.6. Creazione paragrafi §3.3.3.3, §3.4.6.4, §3.4.6.5, §3.5.7. Rimozione dei casi d'uso FEQ (OID 1.3.6.1.4.1.48990.1.1.9.4: §3.1.4, §3.2.2.3, §3.2.3.5, §3.3.2.3, §3.3.3.3, §3.3.4.3, §3.4.3, §3.5.4 della v1.5) ed eMRTD (OID 1.3.6.1.4.1.48990.1.1.9.7: §3.1.7, §3.2.2.6, §3.2.3.3, §3.3.4.6,	1.6	10/11/26	D.Saccò	F.Barcellini	P.Sironi

Sommario

1 INTRODUZIONE 8

1.1 Quadro generale 8

1.2 Nome e identificazione del documento 9

1.3 Livello di Garanzia 10

1.4 Partecipanti IPSP 10

1.4.1 Intesi Group come Fornitore di Servizi di Verifica dell'Identità 10

1.4.2 Prestatore di Servizi Fiduciari Qualificati 11

1.4.3 Soggetto o Richiedente 11

1.4.4 Registration Officer o Operatore di Back Office 11

1.4.5 Azienda del Registration Officer 11

1.4.6 External Identity Proofing Service Provider (External IPSP) 12

1.4.7 Altri partecipanti 12

1.5 Amministrazione del IPSPS 12

1.6 Definizione e acronimi 12

2 PUBBLICAZIONE 13

2.1 Informazioni pubblicate 13

2.2 Data e frequenza delle pubblicazioni 13

2.3 Accesso 13

3 VERIFICA DELL'IDENTITA' 14

3.1 Tipologie di identificazione (Casi d'uso) 14

3.1.1 In presenza (Caso d'uso 9.2.1.2 in [4]) 14

3.1.2 Da remoto non assistita (Caso d'uso 9.2.3.3 in [4]) 15

3.1.3 Tramite eID con livello di garanzia “elevato” (Caso d'uso 9.2.4 in [4]) 15
3.1.4 Persone Giuridiche (Caso d'uso 9.3 in [4]) 15
3.1.5 Persona Fisica che rappresenta una Persona Giuridica (Caso d'uso 9.4 in [4]) ... 16
3.2 Fase preliminare 17
3.2.1 Informazione e consenso..... 17
3.2.2 Mezzi di identificazione richiesti 17
3.2.3 Strumenti tecnologici 19
3.2.4 Accessibilità per persone con disabilità (eIDAS Art. 15)..... 20
3.3 Raccolta dati del Richiedente 21
3.3.1 Dati raccolti..... 21
3.3.2 Prove di identità accettate 23
3.3.3 Modalità di acquisizione dei dati..... 24
3.3.4 Freshness 25
3.4 Validazione generale dei dati..... 28
3.4.1 Validazione identificazione fisica o remota (Casi d’uso 3.1.1 e 3.1.2) 28
3.4.2 Validazione eID (Caso d’uso 3.1.3) 30
3.4.3 Validazione della persona giuridica (Caso d’uso 3.1.4) 31
3.4.4 Validazione Persona Fisica rappresentante Persona Giuridica (Caso d’uso 3.1.5)31
3.4.5 Controlli Antifrode (Tutti i casi d’uso) 31
3.4.6 Validazione tramite registri fiduciari e fonti autorevoli 32
3.4.7 Validazione tramite Proof of Access dei recapiti..... 35
3.4.8 Sistema tecnologico di acquisizione delle evidenze e controlli automatizzati 36
3.5 Binding al Richiedente 41

3.5.1 Binding nella identificazione in presenza (Caso d'uso 3.1.1) 41
3.5.2 Binding nella identificazione da remoto (Caso d'uso 3.1.2) 42
3.5.3 Binding tramite eID notificati (Caso d'uso 3.1.3) 42
3.5.4 Binding Persona Giuridica (Caso d'uso 3.1.4) 43
3.5.5 Binding Persona Fisica rappresentante Persona Giuridica (Caso d'uso 3.1.5) 43
3.5.6 Gestione delle discrepanze 43
3.5.7 Confronto del volto da parte del Registration Officer 43
3.6 Rilascio del risultato 44
3.6.1 Tipologia di esito 44
3.6.2 Raccolta e conservazione delle prove 45
4 CONTROLLI DI GESTIONE 46
4.1 Valutazione dei rischi operativi 46
4.2 Analisi e monitoraggio delle minacce 46
4.3 Controlli di sicurezza del personale 47
4.3.1 Selezione e affidabilità 47
4.3.2 Formazione specialistica 47
4.3.3 Aggiornamento e riqualificazione 48
4.3.4 Separazione dei ruoli 48
4.4 Sicurezza fisica e logica 48
4.4.1 Sicurezza fisica 48
4.4.2 Sicurezza logica e separazione dei sistemi 49
4.4.3 Protezione delle comunicazioni e dei dati 49
4.5 Gestione degli incidenti e delle vulnerabilità 49

4.5.1 Monitoraggio e rilevamento 50
4.5.2 Analisi delle vulnerabilità 50
4.5.3 Obblighi di comunicazione 50
4.5.4 Comunicazione agli interessati 50
4.6 Registrazione degli Audit e conservazione delle prove 50
4.6.1 Tipologia di eventi e evidenze raccolte 51
4.6.2 Periodo di conservazione 51
4.6.3 Sicurezza e Integrità 52
4.7 Continuità operativa e cessazione 52
4.7.1 Piani di Continuità Operativa e Disaster Recovery 52
4.7.2 Terminazione del Servizio 52
4.8 Gestione dei fornitori (Supply-chain) 53
4.8.1 Responsabilità 53
4.8.2 Valutazione e Monitoraggio 53
4.8.3 Accordi Contrattuali 53
5 CONDIZIONI GENERALI DI SERVIZIO 54
5.1 Tariffe del servizio 54
5.2 Responsabilità finanziaria e assicurazioni 54
5.3 Privacy e protezione dei dati personali 54
5.4 Diritti di proprietà intellettuale 54
5.5 Limiti di responsabilità 55
5.6 Reclami, risoluzione delle dispute e legge applicabile 55

1 INTRODUZIONE

1.1 Quadro generale

Il presente Manuale Operativo (IPSPS) descrive il servizio di verifica delle identità delle persone fisiche denominato IG Persona. Questo servizio è offerto da Intesi Group S.p.A. in qualità di fornitore di Servizi Fiduciari Qualificati per l'identificazione dei soggetti destinatari del servizio.

In particolare vengono descritti i requisiti tecnici, di sicurezza e di organizzazione adottati da Intesi Group S.p.A. che rendono la soluzione conforme al regolamento (UE) 2024/1183 del parlamento europeo e del consiglio dell'11 aprile 2024 per quanto riguarda l'istituzione del quadro europeo per l'identità digitale, che modifica 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.

Il presente IPSPS non intende costituire un CPS ai sensi di RFC 3647, ma adotta tale struttura come riferimento metodologico per la descrizione del servizio di *Identity Proofing*.

Il presente documento integra il manuale operativo dei servizi fiduciari pubblicato sul sito Intesi Group:

[1] TSPPS Trust Service Practice Statement

La soluzione IG Persona soddisfa i requisiti previsti dai seguenti standard:

[2] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[3] ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
[4] ETSI TS 119 461 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
[5] ETSI TS 119 471 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services.

1.2 Nome e identificazione del documento

Questo documento è intitolato “Identity Proofing Service Practice Statement”.

Nome e versione sono indicati anche nel frontespizio.

Gli Object Identifier (OID) a cui è associato il documento vengono elencati nella tabella seguente, contenente anche le descrizioni delle politiche utilizzate per ciascun metodo di identificazione adottato:

Intesi OID (Object Identifier)	Descrizione
1.3.6.1.4.1.48990.1.1.9.1	Caso d’uso relativo alla verifica presidiata dell’identità del richiedente mediante documento fisico, effettuata in presenza del richiedente e valutata da un operatore incaricato (RAO), in conformità ai requisiti della norma ETSI TS 119 461 descritti nel paragrafo 9.2.1.2.
1.3.6.1.4.1.48990.1.1.9.2	Casi d’uso che prevedono l’utilizzo di un documento fisico per la verifica remota non presidiata dell’identità, con funzionamento ibrido manuale e automatizzato (Conforme ai requisiti della norma ETSI TS 119 461 descritti nel paragrafo 9.2.3.3)
1.3.6.1.4.1.48990.1.1.9.3	Casi d’uso che prevedono l’identificazione tramite autenticazione con mezzi di identificazione elettronica (eID) notificati con livello di garanzia "Elevato" (SPID Livello 3 e CIE). (Conforme ai requisiti della norma ETSI TS 119 461 descritti nel paragrafo 9.2.4 e nell'Allegato C.3.2).
1.3.6.1.4.1.48990.1.1.9.5	Casi d’uso per la verifica dell'identità di una persona giuridica per il rilascio di certificati qualificati di sigillo elettronico, al livello Extended LoIP (conforme ai requisiti ETSI TS 119 461 del paragrafo 9.3 e dell’Allegato C, clausola C.3.5).

1.3.6.1.4.1.48990.1.1.9.6	Casi d'uso per la verifica dell'identità di una persona fisica che rappresenta una persona giuridica per il rilascio di certificati qualificati di firma elettronica con ruolo, al livello Extended LoIP (Conforme ai requisiti della norma ETSI TS 119 461 descritti nel paragrafo 9.4 e dell'Allegato C, clausola C.3.6).

1.3 Livello di Garanzia

Il livello di garanzia raggiunto dalle procedure che compongono la soluzione IG Persona è elevato (Extended LoIP) e viene descritto dal seguente Object Identifier ETSI:

ETSI OID (Object Identifier)	**Livello di garanzia**
0.4.0.19461.1.2	Extended Level of Identity Proofing (Extended LoIP)

1.4 Partecipanti IPSP

Intesi Group S.p.A. è un fornitore di servizi fiduciari ed utilizza, laddove previsto, la procedura di verifica dell'identità delle persone fisiche secondo le modalità descritte nel presente IPSPS. Le presenti procedure sono utilizzate anche per il rilascio dell'identità digitale SPID.

Tutti i servizi offerti sono erogati da Intesi Group tramite infrastrutture ospitate in data center ad elevato livello di sicurezza. La collocazione e le caratteristiche costruttive delle strutture che ospitano servizi e apparecchiature sono adeguate alla gestione e alla protezione di informazioni sensibili e di alto valore.

1.4.1 Intesi Group come Fornitore di Servizi di Verifica dell'Identità

Intesi Group è Fornitore di Servizi di Verifica dell'Identità, e si identifica nel seguente modo:

Nome della società: Intesi Group S.p.A.

Sede Legale: Via Torino, 48 – 20123 Milano (MI) – ITALIA

Rappresentante Legale: Paolo Sironi (Consiglio di Amministrazione)

Partita IVA e Codice Tributario: IT02780480964

Telefono: +39 02 6760641

Identificatore di Oggetto ISO (OID): 1.3.6.1.4.1.48990

Sito web della società: http://www.intesigroup.com

Indirizzo e-mail della società: intesi@intesigroup.com

1.4.2 Prestatore di Servizi Fiduciari Qualificati

È Intesi Group in qualità di QTSP che gestisce il processo ed eroga servizi fiduciari.

1.4.3 Soggetto o Richiedente

La persona fisica richiedente il servizio, che deve essere sottoposta all'identificazione.

Nel caso di persone giuridiche e di persone fisiche che le rappresentano (§3.1.4 e §3.1.5), il Richiedente è la persona fisica identificata, indicata nel modulo di autorizzazione come delegato o come soggetto per cui il terzo interessato richiede il certificato. Il Sottoscrittore è il legale rappresentante dell'ente o, per il sigillo elettronico, un procuratore con poteri di firma, che sottoscrive il modulo di autorizzazione e allega il documento che comprova la propria carica o i propri poteri (§3.2.2). Il Sottoscrittore non è il Richiedente, salvo che le due persone coincidano.

1.4.4 Registration Officer o Operatore di Back Office

Personale appositamente formato che esegue le procedure manuali del processo di verifica dell'identità, esamina i risultati di convalida e verifica il collegamento fra la persona e il documento di identità presentato (binding manuale del Soggetto). Può essere personale interno di Intesi Group o appartenente ad una società a cui Intesi Group subappalta il servizio di identificazione.

1.4.5 Azienda del Registration Officer

Azienda di appartenenza del Registration Officer, subappaltatrici del servizio di identificazione. Queste aziende devono appartenere alla catena di fornitura di Intesi Group.

1.4.6 External Identity Proofing Service Provider (External IPSP)

Intesi Group può avvalersi di fornitori esterni specializzati che offrono servizi di identity proofing all'interno della propria supply chain ICT. Tali soggetti forniscono componenti tecnologiche e operative per la verifica dell'identità remota. In questo modello, Intesi Group mantiene la piena responsabilità legale e operativa (accountability) dell'intero processo verso l'organismo di vigilanza (AgID) e i CAB

1.4.7 Altri partecipanti

Le attività svolte dal QTSP Intesi Group sono soggette alla supervisione di AgID (Agenzia per l'Italia Digitale).

1.5 Amministrazione del IPSPS

Il presente IPSPS viene redatto, revisionato, e aggiornato da personale appositamente incaricato di Intesi Group S.p.A. e viene pubblicato solamente dopo essere stato approvato dalla Direzione di Intesi Group e dall'Agenzia per l'Italia Digitale. Richieste di informazioni o chiarimenti riguardo al presente IPSPS possono essere inviate scrivendo una e-mail all'indirizzo **tsp@intesigroup.com.**

1.6 Definizione e acronimi

Acronimi	Definizione
eIDAS2	Regolamento (UE) 2024/1183 del parlamento europeo e del consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo ad un'identità digitale.
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
RO	Registration Officer
RFC	Request For Comments
TLS	Transport Layer Security
TSP	Trust Service Provider

Acronimi	Definizione
TSPP	TSP Policy
IPSPS	IPS Practice Statement
LoA	Level of assurance
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OID	Object Identifier
PAD	Presentation Attack Detection
VIZ	Visual Inspection Zone

2 PUBBLICAZIONE

2.1 Informazioni pubblicate

Questo documento è reso pubblico attraverso il sito web istituzionale di Intesi Group (https://www.intesigroup.com/it/qtsp/documenti/) e pubblicato in copia sul sito web di AgID (http://www.agid.gov.it/).

2.2 Data e frequenza delle pubblicazioni

La frequenza di pubblicazione e aggiornamento della documentazione è stabilita da processi interni di Intesi Group. La versione da ritenersi valida è l'ultima versione disponibile presente sul sito web del servizio di certificazione (www.intesigroup.com) oppure, dove applicabile, quella pubblicata sul sito web di AgID (www.agid.gov.it).

2.3 Accesso

L'accesso alla documentazione è libero e non richiede autenticazione.

3 VERIFICA DELL'IDENTITA'

Al fine di elevare il livello di sicurezza dei processi di identificazione e proteggersi dai principali attacchi (Presentation attacks, Injection attacks, Deepfake), Intesi Group utilizzando l'esperienza maturata sul campo negli ultimi anni, ha sviluppato un nuovo sistema di identificazione chiamato *IG Persona*.

3.1 Tipologie di identificazione (Casi d'uso)

Il servizio IPSP implementa il processo di verifica dell'identità articolandolo nelle seguenti cinque fasi fondamentali:

- fase preliminare;
- raccolta dei dati;
- validazione;
- binding al richiedente;
- rilascio del risultato.

Le tipologie di identificazione del servizio di *Identity Proofing* del servizio Intesi Group, che garantiscono l'**Extended Level of Identity Proofing (LoIP)** sono quelle indicate nel paragrafo 1.2 e descritte di seguito.

Per i casi d'uso di identificazione remota non assistita (§3.1.2), e identificazione in presenza (§3.1.1) la gestione automatizzata delle deviazioni (es. qualità dell'evidenza insufficiente, discrepanze tra fonti) e le relative condizioni di interruzione (abort) del processo sono disciplinate ai §3.4.6.3 (Gestione delle discrepanze), §3.4.8.2 (Controlli della sessione di acquisizione remota), §3.5.6 (Gestione delle discrepanze in fase di binding) e §3.6.1 (Tipologia di esito).

3.1.1 In presenza (Caso d'uso 9.2.1.2 in [4])

Verifica con presenza fisica del richiedente, basata su:

- esame del documento di identità fisico presentato dal richiedente da parte del Registration Officer, inclusa la verifica della corrispondenza tra il richiedente e il titolare del documento e l'analisi degli elementi di sicurezza visibili del documento;
- binding manuale tra il soggetto identificato e il documento di identità da parte del Registration Officer;

- integrazione della verifica presidiata con controlli automatizzati documentali, biometrici e antifrode previsti dalle procedure del QTSP.

3.1.2 Da remoto non assistita (Caso d'uso 9.2.3.3 in [4])

Verifica remota non assistita (ibrida), basata su:

- raccolta automatizzata di prove di identità;
- acquisizione video in tempo reale;
- validazione sicurezza biometrica (rilevamento attacchi PAD e rilevamento iniezione IAD)
- validazione automatizzata di documenti (scansione OCR e analisi AI/Machine learning);
- binding tra Richiedente e documento mediante tecnologie biometriche e revisione manuale.

3.1.3 Tramite eID con livello di garanzia “elevato” (Caso d'uso 9.2.4 in [4])

Verifica dell’identità mediante sistemi di identificazione elettronica notificati (eID Means) ai sensi del Regolamento eIDAS, con livello di garanzia “Elevato” (eIDAS High), basata sui seguenti controlli:

- autenticazione del Richiedente tramite un Identity Provider (IdP) qualificato, ad esempio SPID Livello 3;
- in alternativa, lettura del microchip NFC della Carta d’Identità Elettronica (CIE);
- acquisizione dell’asserzione di autenticazione contenente gli attributi identificativi certificati;
- verifica dell’integrità, dell’autenticità e della validità dell’asserzione ricevuta;
- associazione univoca tra la sessione IPSP e l’identità autenticata.

Nel caso di identificazione tramite EUDI Wallet, vengono acquisiti i Person Identification Data (PID) mediante il protocollo previsto, verificando che gli stessi siano associati a un livello di garanzia LoA High e che soddisfino i requisiti di validità, autenticità e non revoca previsti.

L’identificazione tramite EUDI Wallet è predisposta ma non è attiva alla data di emissione del presente documento. Sarà attivata solo quando saranno disponibili PID rilasciati da PID Provider autorizzati, previo aggiornamento del presente IPSPS e delle relative informazioni pubblicate (OID).

3.1.4 Persone Giuridiche (Caso d'uso 9.3 in [4])

Verifica dell’identità di una **persona giuridica**, finalizzata all’emissione di certificati qualificati di sigillo elettronico, al livello Extended LoIP, basata su:

- acquisizione di prove di identità dell'organizzazione provenienti da fonti autorevoli e indipendenti (es. visura camerale, registri pubblici ufficiali, Camera di Commercio o registri equivalenti);
- verifica dell'esistenza legale dell'organizzazione presso il registro ufficiale competente;
- acquisizione e verifica dei principali attributi identificativi dell'ente, tra cui almeno:
  - denominazione sociale completa;
  - indirizzo della sede legale;
  - numero di registrazione ufficiale dell'organizzazione (es. Partita IVA, Codice Fiscale o identificativo equivalente);
- verifica della coerenza e validità delle informazioni raccolte da parte del Registration Officer, rispetto alle fonti ufficiali consultate;
- identificazione della persona fisica che presenta la richiesta per conto dell'organizzazione, al livello Extended LoIP, la cui identità deve essere verificata mediante una delle modalità di identificazione previste nei paragrafi da 3.1.1 a 3.1.3.

La verifica della documentazione dell'ente è effettuata dal RAO nel corso dell'identificazione del Richiedente

3.1.5 Persona Fisica che rappresenta una Persona Giuridica (Caso d'uso 9.4 in [4])

Verifica dell'identità di una persona fisica che agisce per conto di una persona giuridica, finalizzata al rilascio di servizi fiduciari associati all'organizzazione (es. certificati di firma con ruolo aziendale o altri certificati qualificati), basata su:

- identificazione della persona fisica richiedente mediante una delle modalità previste per le persone fisiche (paragrafi da 3.1.1 a 3.1.3), garantendo un livello di affidabilità conforme all'Extended Level of Identity Proofing (LoIP);
- acquisizione e verifica della documentazione attestante il rapporto tra la persona fisica e l'organizzazione per conto della quale viene presentata la richiesta;
- verifica dei poteri di rappresentanza o autorizzazione del richiedente tramite documentazione probatoria emessa da fonti autorevoli come uno dei documenti indicati al §3.3.2;;
- verifica della validità, integrità e coerenza della documentazione presentata, nonché della persistenza dei poteri di rappresentanza al momento della richiesta;
- associazione tra l'identità verificata della persona fisica e l'organizzazione rappresentata, con registrazione delle evidenze utilizzate ai fini di audit.

Le verifiche relative ai poteri di rappresentanza possono essere effettuate mediante consultazione diretta di registri pubblici ufficiali, quando disponibili, oppure tramite documentazione fornita dal richiedente e successivamente validata dal personale autorizzato di Intesi Group.

3.2 Fase preliminare

La fase preliminare è gestita dal RAO nell'identificazione in presenza e da IG Persona nell'identificazione da remoto e con eID. In questa fase il Richiedente è informato sul processo di identificazione, sul suo scopo e sulle condizioni applicabili, e deve fornire il consenso esplicito ai termini e alle condizioni prima dell'avvio della verifica. Per le persone giuridiche e per i loro rappresentanti la fase preliminare è quella del caso d'uso scelto per l'identificazione del Richiedente.

3.2.1 Informazione e consenso

Prima di iniziare il processo di identificazione, il Richiedente è informato sullo scopo della verifica e deve accettare attivamente i termini e le condizioni del servizio. Questa sezione include l'informativa sulla protezione dei dati personali in conformità al GDPR, specificando quali informazioni saranno raccolte e le finalità del trattamento. Nei casi d'uso che prevedono il riconoscimento del volto o il binding biometrico, viene acquisito il consenso esplicito del Richiedente prima del trattamento dei dati biometrici.

3.2.2 Mezzi di identificazione richiesti

Ai fini dell'identificazione, il Richiedente viene informato preventivamente sui mezzi di identificazione richiesti in base al caso d'uso selezionato.

3.2.2.1 Identificazione fisica o remota

Si rende obbligatoria la presentazione di un documento di riconoscimento che sia:

- in corso di validità;
- in originale (non è possibile caricare immagini o video effettuati in precedenza);
- di proprietà della persona che effettua l'identificazione.

3.2.2.2 Identificazione per mezzo di eID notificati di livello Elevato

Per avviare l'identificazione mediante mezzo di identificazione elettronica notificato con livello di garanzia "elevato" ai sensi del Regolamento (UE) n. 910/2014 (eIDAS), il Richiedente deve disporre di:

- un mezzo di identificazione elettronica notificato con livello di garanzia elevato, rilasciato da uno Stato membro dell'Unione Europea;
- credenziali valide e attive associate al mezzo eID;
- eventuali strumenti di autenticazione richiesti dal sistema eID (es. dispositivo fisico, PIN, applicazione dedicata).

Il Richiedente deve inoltre utilizzare un dispositivo compatibile con il sistema di autenticazione previsto dal mezzo eID e disporre di una connessione Internet attiva per completare il processo.

L'accesso al servizio è subordinato al buon esito dell'autenticazione presso l'Identity Provider del sistema eID notificato.

Nel caso in cui l'identificazione del richiedente avvenga tramite EUDI Wallet, il richiedente deve disporre di un dispositivo sul quale sia installata un'applicazione Wallet rilasciata o riconosciuta da uno Stato membro dell'Unione Europea.

All'interno del Wallet devono essere presenti Person Identification Data (PID) con livello di garanzia (Level of Assurance – LoA) pari a "High".

L'identificazione tramite EUDI Wallet è predisposta ma non è attiva alla data di emissione del presente documento. Sarà attivata solo quando saranno disponibili PID rilasciati da PID Provider autorizzati, previo aggiornamento del presente IPSPS e delle relative informazioni pubblicate (OID).

3.2.2.3 Identificazione di persona giuridica

Nel caso di identificazione di una persona giuridica, il Richiedente deve fornire documentazione idonea a dimostrare l'esistenza legale dell'organizzazione e i relativi dati identificativi.

Il Richiedente carica in autonomia su IG Persona il modulo di autorizzazione alla richiesta del sigillo elettronico qualificato, compilato e firmato dal legale rappresentante dell'ente o da un procuratore con poteri di firma (Sottoscrittore), con uno dei documenti elencati al §3.3.2.

3.2.2.4 Identificazione di persona fisica che rappresenta una persona giuridica

Nel caso in cui il Richiedente agisca per conto di una persona giuridica, oltre ai mezzi di identificazione previsti per le persone fisiche, deve essere fornita documentazione idonea a dimostrare il rapporto tra il Richiedente e l'organizzazione rappresentata.

Il Richiedente carica in IG Persona il modulo di autorizzazione, firmato e timbrato dal legale rappresentante dell'ente (Sottoscrittore), con uno dei documenti elencati al §3.3.2. Il modulo dichiara che il Richiedente appartiene o è affiliato all'ente e, se si vuole l'attributo Title, ne indica il ruolo.

3.2.3 Strumenti tecnologici

Il processo di identificazione richiede l'utilizzo di strumenti tecnologici idonei a garantire l'affidabilità e la qualità della verifica, in funzione della modalità di identificazione selezionata.

3.2.3.1 Dispositivo

Il Richiedente deve disporre di un dispositivo (PC, smartphone o tablet) compatibile con il servizio, adeguatamente configurato e dotato dei requisiti tecnici necessari alla specifica modalità di identificazione scelta.

3.2.3.2 Acquisizione immagini e video (ove prevista)

Nei casi di identificazione fisica o remota basata su documento, Il dispositivo utilizzato per l'identificazione deve essere dotato di una fotocamera con risoluzione minima di 1280x720 pixel (HD) e deve essere in grado di catturare un flusso video in tempo reale con una frequenza di almeno 25 fps (frame per secondo). Inoltre, il dispositivo deve supportare la messa a fuoco automatica e garantire la stabilità dell'immagine per consentire la corretta lettura dei documenti e l'analisi biometrica del volto.

Il servizio non consente l'utilizzo di immagini, registrazioni o file pre-acquisiti; ove prevista l'acquisizione di dati biometrici o documentali, essa deve avvenire in tempo reale durante la sessione di identificazione.

3.2.3.3 Autenticazione tramite eID notificato

Per l'identificazione mediante mezzo di identificazione elettronica notificato con livello di garanzia elevato (LoA High), il dispositivo deve essere compatibile con il sistema di autenticazione previsto dal mezzo eID utilizzato.

3.2.3.4 Connettività

È richiesta una connessione Internet attiva e stabile, tale da consentire il completamento del processo senza interruzioni che possano comprometterne la validità.

3.2.4 Accessibilità per persone con disabilità (eIDAS Art. 15)

In conformità all'Articolo 15 del Regolamento (UE) n. 910/2014 (eIDAS) e ai requisiti della norma ETSI TS 119 461, Intesi Group adotta misure atte a garantire l'accesso ai servizi di identificazione anche ai Richiedenti con disabilità, assicurando la disponibilità di modalità alternative equivalenti e prevenendo situazioni di discriminazione.

3.2.4.1 Accessibilità della soluzione tecnologica

Il servizio IG Persona si basa su una piattaforma tecnologica (rif par. 3.4.8.1), sviluppata considerando i principi delle linee guida WCAG (Web Content Accessibility Guidelines), con l'obiettivo di supportare l'accessibilità delle funzionalità principali del processo di identificazione, laddove tecnicamente applicabile.

Tuttavia, alcune fasi del processo di identificazione automatizzata o ibrida (es. acquisizione biometrica del volto, corretto posizionamento del documento) possono risultare non pienamente accessibili per specifiche categorie di utenti (es. soggetti con disabilità visive o motorie).

3.2.4.2 Procedura operativa di gestione

Qualora il Richiedente non sia in grado di completare uno dei processi di identificazione, può richiedere assistenza tramite i canali di supporto messi a disposizione da Intesi Group.

Le richieste di supporto sono gestite tramite il sistema di ticketing aziendale.

Il Personale di Supporto, ricevuta una segnalazione di inaccessibilità, segue i seguenti step:

1. **Analisi (SLA 72h):** l'operatore identifica la barriera funzionale riscontrata (es. difficoltà nel posizionamento del documento o nella cattura biometrica).
2. **Valutazione Tecnica:** si verifica se l'utente dispone dei mezzi per un percorso alternativo (es. possesso di SPID o disponibilità a recarsi presso una LRA).

3. **Risoluzione:** l'operatore abilita manualmente il profilo di identificazione idoneo tra quelli descritti al par. 3.2.4.3 e guida l'utente nel nuovo flusso.

3.2.4.3 Modalità alternative di identificazione

In tali circostanze, il Richiedente può essere indirizzato verso modalità alternative che garantiscono un livello di affidabilità equivalente, tra cui:

- Identificazione tramite mezzo di identificazione elettronica notificato con livello di garanzia "elevato" (rif. par. 3.1.3), che consente una verifica basata su identità digitale già validata, riducendo la necessità di interazioni visive complesse;
- Identificazione in presenza (de visu assistita) (rif. par. 3.1.1), presso una Local Registration Authority (LRA), con il supporto di un Registration Officer.

3.3 Raccolta dati del Richiedente

Il presente capitolo descrive le tipologie di dati personali e documentali raccolti nel corso del processo di identificazione del Richiedente, nonché le modalità con cui tali dati sono acquisiti e utilizzati ai fini della verifica dell'identità.

La raccolta dei dati è limitata a quanto strettamente necessario per garantire l'affidabilità del processo di identity proofing e il rispetto dei requisiti normativi applicabili.

3.3.1 Dati raccolti

I dati del Richiedente che vengono raccolti durante il processo di identificazione, possono variare in funzione della tipologia di identificazione e di documento acquisito e del relativo modello di riferimento. Nel caso di richieste presentate per conto di una persona giuridica, possono essere raccolti anche dati relativi all'organizzazione e alla relazione di rappresentanza. I seguenti dati elencati nei seguenti paragrafi vengono sempre richiesti per raggiungere LoIP High.

3.3.1.1 Dati Anagrafici

- Nome;
- Cognome;

- Data e luogo di nascita;
- Nazionalità
- Codice fiscale o codice identificativo equivalente in base alla nazionalità
- Estremi del documento di identità
- Indirizzo di residenza.

Il Codice fiscale per gli italiani e gli estremi del documento di identità per tutte le persone identificate consentono di identificare univocamente la persona.

3.3.1.2 Dati di contatto

- Numero di telefono (validato tramite invio OTP);
- E-mail (validato tramite invio OTP).

3.3.1.3 Dati della persona giuridica (se applicabile)

Nel caso di identificazione di una persona giuridica o di richiesta effettuata da un soggetto che agisce per conto di un'organizzazione, vengono raccolti i seguenti dati dell'ente:

- Denominazione sociale completa;
- Indirizzo della sede legale;
- Numero di registrazione ufficiale dell'organizzazione (es. Partita IVA, Codice Fiscale o identificativo equivalente);
- Paese di registrazione.

3.3.1.4 Dati relativi alla rappresentanza (se applicabile)

Nel caso in cui il Richiedente agisca per conto di una persona giuridica, vengono raccolte informazioni relative al rapporto tra il Richiedente e l'organizzazione rappresentata, quali:

- ruolo o qualifica del Richiedente nell'organizzazione;
- estremi della documentazione attestante i poteri di rappresentanza (es. visura camerale, procura notarile, delega formale).

3.3.1.5 Dati dell'evidenza

- Dati del documento fisico: tipologia del documento, nazionalità, data di emissione, data di scadenza, paese di emissione, autorità emittente;Dati della sessione eID: asserzione di identità (SAML/JWT) ricevuta.

3.3.2 Prove di identità accettate

In conformità all'Art. 24 del Regolamento eIDAS e alla norma ETSI TS 119 461, sono accettate le seguenti prove.

3.3.2.1 Documenti fisici

Il servizio accetta esclusivamente documenti di riconoscimento:

- rilasciati da autorità governative affidabili;
- contenenti una fotografia del volto del titolare.

In particolare, i documenti accettati sono:

- Carta d'identità Elettronica (CIE);
- Passaporto;
- Patente di guida (per i soli cittadini italiani).

Per i soli cittadini italiani, e limitatamente ai riconoscimenti di tipo LoIP Extended, è inoltre richiesta la tessera sanitaria, al fine di consentire la verifica del codice fiscale e della validità del documento.

3.3.2.2 Mezzi eID

Credenziali di sistemi di identità digitale notificati a livello UE (es. SPID, CIE per l'Italia) con livello di garanzia 'Elevato' ai sensi del Regolamento eIDAS, rilasciate secondo procedure conformi agli standard applicabili per garantire affidabilità comparabile all'Extended LoIP.

3.3.2.3 Evidenze relative alla persona giuridica

Nel caso di identificazione di una persona giuridica o di verifica dei poteri di rappresentanza, il servizio accetta evidenze provenienti da registri pubblici ufficiali o da autorità competenti, tra cui:

- Statuto;
- atto costitutivo;
- procura notarile;
- estratto di atto notarile;
- certificato o visura della Camera di Commercio;
- per le pubbliche amministrazioni, legge o atto istitutivo.

L'esistenza dell'ente è verificata dal RAO sui registri ufficiali (§3.4.6); la carica o i poteri di firma del Sottoscrittore sono verificati sul documento allegato.

Tali evidenze sono utilizzate per verificare:

- l'esistenza legale dell'organizzazione;
- i dati identificativi dell'ente;
- i poteri di rappresentanza del Richiedente.

3.3.3 Modalità di acquisizione dei dati

A seconda della modalità di identificazione scelta, la raccolta dei dati avviene con le seguenti modalità:

3.3.3.1 Scansione OCR e Biometria (Casi d'uso 3.1.1 e 3.1.2)

L'acquisizione delle immagini:

- del documento di identità
- del volto del richiedente
- della sessione video (ove prevista)

finalizzata alla liveness detection e alla verifica di corrispondenza biometrica tra il soggetto e la fotografia presente sul documento, avviene mediante fotocamera integrata nello smartphone.

In caso di identificazione da remoto, il richiedente deve essere in possesso di uno smartphone dotato di fotocamera funzionante, connesso a Internet e compatibile con l'applicativo di identificazione. In caso di identificazione in presenza, l'acquisizione è effettuata tramite il dispositivo in dotazione al Registration Officer.

Il dispositivo deve garantire una qualità di acquisizione tale da consentire la corretta lettura del documento e l'analisi biometrica del volto (risoluzione, messa a fuoco automatica, stabilità dell'immagine).

La raccolta dei dati avviene secondo le seguenti modalità:

- Scansione OCR: le immagini vengono acquisite tramite interfaccia guidata e i dati estratti tramite riconoscimento ottico dei caratteri; il caricamento di file pre-esistenti (upload) è vietato per prevenire frodi.
- Selfie: per l'identificazione in presenza, viene acquisita tramite device mobile una fotografia del volto del richiedente ai fini dei controlli biometrici successivi alla verifica effettuata dal Registration Officer. Anche in questo caso non è possibile il caricamento di fotografie pre-esistenti.
- Interazione Video: per l'identificazione da remoto, viene catturato un flusso video del volto del richiedente per la verifica di liveness e per il successivo binding biometrico con la fotografia del documento.

3.3.3.2 Autenticazione Digitale (Caso d'uso 3.1.3)

L'acquisizione dei dati è automatizzata tramite la ricezione di un'asserzione SAML (o equivalente) dall'Identity Provider a seguito di autenticazione forte del Richiedente. Questa modalità sostituisce l'acquisizione visiva del documento.

3.3.3.3 Persone giuridiche e rappresentanti (Casi d'uso 3.1.4 e 3.1.5)

L'acquisizione dei dati del Richiedente in quanto persona fisica segue quanto descritto nei paragrafi 3.3.3.1 e 3.3.3.2. Il modulo di autorizzazione e il documento allegato (§3.3.2) sono caricati direttamente dal Richiedente in IG Persona.

3.3.4 Freshness

In conformità ai requisiti della norma ETSI TS 119 461, Intesi Group applica una politica di verifica della "freschezza" delle prove raccolte in base al contesto di identity proofing e al livello di affidabilità (LoIP) richiesto, per garantire che gli attributi identificativi siano attuali e affidabili al momento dell'identificazione. Per i servizi che richiedono l'Extended LoIP, vengono adottati criteri più stringenti per mitigare i rischi associati ad avversari con alto potenziale di attacco. Nei paragrafi successivi vengono descritti i casi specifici.

Caso d'Uso IPSP (§3.1)	**Tipologia di Evidenza Acquisita**	**Requisito di Freschezza (LoIP – Baseline)**	**Requisito di Freschezza (Extended LoIP)**
§3.1.1 In presenza (ETSI 9.2.1.2)	Documento di riconoscimento e foto/selfie del richiedente	Il documento di riconoscimento deve essere in corso di validità al momento della verifica.	Documento in corso di validità con valutazione della foto rispetto all'età del richiedente; acquisizione della foto/selfie in tempo reale.
§3.1.2 Da remoto non assistita (ETSI 9.2.3.3)	Documento di identità, Tessera Sanitaria (solo IT) e flusso video/selfie biometrico	Documento in corso di validità; acquisizione del flusso video/selfie contestuale alla sessione.	Documento in corso di validità con valutazione foto/età e Tessera Sanitaria; acquisizione video in tempo reale con rilevamento attacchi di iniezione (IAD).
§3.1.3 Tramite eID notificato (ETSI 9.2.4)	Asserzione di autenticazione eID (SAML/OIDC) o Person Identification Data (PID)	Asserzione eID generata in tempo reale nel corso della sessione IPSP.	Asserzione eID o PID validati al momento della ricezione, verificando livello eIDAS High, autenticità e assenza di revoca o scadenza.
§3.1.4 Persone Giuridiche (ETSI 9.3)	Visure camerali, certificati da registri pubblici ufficiali	Le evidenze provenienti da fonti autorevoli devono essere state emesse da non oltre **6 mesi**.	Le evidenze provenienti da fonti autorevoli devono essere state emesse da non oltre **3 mesi** (per garantire l'attualità dei poteri).
§3.1.5 Persona Fisica rappresentante Persona Giuridica (ETSI 9.4)	Identità del Rappresentante e Documentazione dei poteri di rappresentanza	Identità valida + Documentazione dei poteri/visura emessa da non oltre **6 mesi**.	Identità verificata con livello Extended LoIP + Documentazione attestante i poteri emessa da non oltre **3 mesi**.

Nota: per l'emissione di certificati qualificati si applica il solo requisito Extended LoIP (ETSI TS 119 461, Allegato C, clausola C.3). I requisiti Baseline sono riportati ai soli fini di completezza.

3.3.4.1 Documenti di identità (Fisici o Digitali)

LoIP – Baseline: il documento deve essere in corso di validità al momento della verifica. Non sono accettati documenti scaduti.

LoIP – Extended: in aggiunta alla verifica di validità al momento della acquisizione, viene effettuata una valutazione della fotografia rispetto all'età del richiedente, in modo da prevenire l'utilizzo di documenti obsoleti.

3.3.4.2 Identità digitali eID

Indipendentemente dal livello di affidabilità, l'asserzione di autenticazione (SAML o equivalente) eseguita tramite eID means deve essere generata in tempo reale nel corso della sessione IPSP. Al momento della ricezione, l'asserzione viene validata verificando l'autenticità della firma e il rispetto dell'intervallo temporale di validità.

Nel caso di Person Identification Data (PID) richiesti tramite EUDI Wallet, i dati vengono validati al momento della ricezione, verificandone la validità, l'assenza di revoca o scadenza, nonché la corretta emissione da parte di un ente nazionale abilitato.

3.3.4.3 Visure Camerali / Registri ufficiali

LoIP – Baseline: le evidenze provenienti da fonti autorevoli per persone giuridiche devono essere state emesse da non oltre 6 mesi.

LoIP – Extended: le evidenze provenienti da fonti autorevoli per persone giuridiche devono essere state emesse da non oltre 3 mesi, per garantire l'attualità dei poteri di rappresentanza.

3.3.4.4 Prove Biometriche (Selfie/Video)

Indipendentemente dal livello di affidabilità, l'acquisizione deve avvenire esclusivamente in tempo reale con rilevamento attacchi di iniezione (IAD). È vietato l'uso di file pre-esistenti.

3.4 Validazione generale dei dati

Il sistema di identificazione di Intesi Group (IG Persona) effettua una validazione strutturata e approfondita di tutti i dati raccolti durante il processo di identity proofing.

Il presente capitolo descrive le principali funzionalità di verifica, controllo e correlazione dei dati, distinguendo i controlli applicati in base al tipo di identificazione.

3.4.1 Validazione identificazione fisica o remota (Casi d'uso 3.1.1 e 3.1.2)

3.4.1.1 Documenti

Il servizio di acquisizione e verifica dei documenti d'identità consente di riconoscerli tra 500 documenti emessi da 190 Paesi diversi.

Attraverso tale servizio vengono:

- acquisite le immagini del documento e verificate le principali caratteristiche di sicurezza (es. inchiostri OVI, microscritture, Kinegram, ologrammi);
- estratti i dati personali del Richiedente tramite OCR;
- estratti i dati personali dalla lettura della componente MRZ (Machine Readable Zone).

Viene inoltre catturata l'immagine del volto dell'utente tramite selfie, utilizzata per i controlli biometrici di confronto con la fotografia presente nel documento.

Sulla base dei dati acquisiti, vengono effettuati i seguenti controlli:

- verifica della data di scadenza del documento;
- verifica della maggiore età dell'utente;
- verifica del checksum del codice MRZ;
- coerenza tra i dati catturati tramite OCR con i dati catturati da MRZ;
- rilevazione di documenti fotocopiati o mostrati a schermo video;
- rilevazione di tentativi di impersonificazione e alterazione della foto stampata;
- rilevamento di documenti generati da intelligenza artificiale (deepfakes) o manipolati digitalmente;
- verifica degli elementi di sicurezza del documento (ologrammi, ecc);

- confronto biometrico 1:1 tra il volto acquisito del richiedente e la fotografia presente nel documento.

La soluzione verifica in tempo reale la qualità dell'immagine (luminosità, contrasto, rumore e riflessi) e, in caso di non conformità ai requisiti minimi, fornisce all'utente indicazioni per una nuova acquisizione.

Per ogni documento fisico acquisito in modalità remota, il sistema verifica sistematicamente almeno 3 caratteristiche di sicurezza, di cui almeno 2 OVD (Optically Variable Devices).

- OVD 1: Inchiostri otticamente variabili (OVI).
- OVD 2: Ologrammi o Kinegram.
- Feature 3: Machine Readable Zone (MRZ) con verifica dei checksum ICAO 9303. L'efficacia di tali controlli è validata dagli score tecnici (es. PrintAttackTest, ReplayAttackTest) restituiti dalla piattaforma.

3.4.1.2 Liveness Detection

Il sistema utilizzata una tecnologia di rilevamento della presenza fisica del soggetto al fine di prevenire attacchi di tipo "Presentation (PAD)" e/o "deepfake". La soluzione è conforme alla norma ISO 30107 ai livelli 1 e 2.

La tecnologia consente di supportare i Registration Officer nella prevenzione dei seguenti attacchi:

- Presentation attacks.
- Video presentation attacks.
- 3D animation attacks.
- Print attacks.
- Mask / 3D photo-mask attacks.
- Mannequin attacks.

La tecnologia "liveness detection" è sottoposta a valutazione e monitoraggio continuo delle prestazioni, in conformità con i criteri definiti nel presente IPSPS.

Per il modulo Active Liveness Detection, il requisito prestazionale di riferimento è maxAPCER < 1% a BPCER = 5%, con un limite superiore di BPCER pari al 15% nell'ambito delle prove eseguite secondo ISO/IEC 19989-3.

Per il modulo Passive Liveness Detection, il requisito prestazionale di riferimento è maxAPCER < 2% a BPCER = 5%.

I moduli di rilevamento della vitalità sono inoltre sottoposti a valutazioni secondo lo standard ISO/IEC 30107 e dispongono di certificazioni iBeta Level 1 e Level 2.

3.4.1.3 Video Identificazione (Solo caso d'uso 3.1.2)

Durante la video identificazione, il sistema registra il Richiedente mentre mostra il fronte e il retro del documento di riconoscimento in un flusso video continuo.

Il video cattura simultaneamente volto e documento, garantendone la sincronizzazione temporale.

Questa modalità consente di:

- dimostrare l'effettivo possesso del documento;
- prevenire attacchi di tipo presentation e injection (IAD).

3.4.2 Validazione eID (Caso d'uso 3.1.3)

Per le identificazioni tramite eID (SPID/CIE o altri sistemi notificati di livello Elevato), la validazione si basa sui controlli automatici effettuati sulla risposta fornita dall'Identity Provider (IdP), mediante:

1. verifica della firma digitale dell'asserzione SAML (o equivalente) rispetto ai certificati pubblicati nei metadati ufficiali;
2. verifica che il livello di autenticazione restituito sia "Elevato" (eIDAS High), quale requisito minimo per il conseguimento dell'Extended LoIP;
3. verifica della presenza e della completezza di tutti gli attributi richiesti.

Per le identificazioni tramite EUDI Wallet, i Person Identification Data (PID) vengono acquisiti dal richiedente mediante il protocollo OID4VP. Alla ricezione, il QTSP effettua i seguenti controlli:

1. verifica della firma dell'issuer del PID rispetto ai certificati e alle informazioni presenti nella Trusted List dello Stato membro competente;
2. verifica della validità e dell'assenza di revoca del PID;
3. verifica del Key Binding, accertando che il presentatore disponga effettivamente delle chiavi associate al Wallet
4. verifica del livello di garanzia LoA High dichiarato nel PID.

L'identificazione tramite EUDI Wallet è predisposta ma non è attiva alla data di emissione del presente documento. Sarà attivata solo quando saranno disponibili PID rilasciati da PID Provider autorizzati, previo aggiornamento del presente IPSPS e delle relative informazioni pubblicate (OID).

3.4.3 Validazione della persona giuridica (Caso d'uso 3.1.4)

Nel corso della verifica dell'identità del Richiedente, il RAO verifica la documentazione relativa all'ente:

1. il modulo di richiesta al §3.2.2 è completo e firmato dal Sottoscrittore;
2. il documento allegato è tra quelli ammessi e rispetta i requisiti di freshness;
3. per gli enti iscritti a un registro, esistenza dell'ente (e, ove riportato dal registro, lo stato), denominazione, sede e identificativo risultano dalla consultazione del registro (§3.4.6) e coincidono con i dati forniti in sede di identificazione;
4. la carica o i poteri di firma del Sottoscrittore risultano dal documento allegato.

3.4.4 Validazione Persona Fisica rappresentante Persona Giuridica (Caso d'uso 3.1.5)

Il Richiedente è identificato con uno dei casi d'uso 3.1.1, 3.1.2 o 3.1.3 al livello Extended LoIP. Il RAO verifica che la persona identificata coincida con quella indicata nel modulo (nome e codice fiscale) e che il Sottoscrittore dichiari che il Richiedente è dipendente o affiliato all'ente.

3.4.5 Controlli Antifrode (Tutti i casi d'uso)

Intesi Group ha sviluppato un componente proprietario di *Anti-fraud detection* che interviene in tutti i casi d'uso integrando i controlli documentali, biometrici o digitali con verifiche di coerenza interna ed esterna. Oltre a quanto già descritto, per i flussi digitali, il sistema verifica:

- verifica in black list interne di:
  - codice fiscale;
  - numero di telefono.
  - Indirizzo e-mail e/o dominio e-mail.
  - documento di riconoscimento.

- controlli di univocità:
  - coppia codice fiscale / indirizzo e-mail.
  - coppia codice fiscale / numero di telefono.
- Verifiche “Scipafi” (solo per cittadini italiani).

3.4.6 Validazione tramite registri fiduciari e fonti autorevoli

In conformità ai requisiti ETSI VAL-8.3.6, Intesi Group utilizza l'accesso al “Sistema centralizzato per la prevenzione del furto d'identità” denominato SCIPAFI, utilizzato per la verifica della validità dei documenti di identità dei cittadini italiani e per la prevenzione dei furti di identità. L’utilizzo delle fonti è limitato ai dati strettamente necessari al completamento del processo di identificazione.

3.4.6.1 Elenco dei registri e delle fonti

In funzione del contesto di identificazione, vengono consultate le seguenti fonti:

Persona fisica: per la verifica dei documenti di identità dei cittadini italiani e per la prevenzione dei furti di identità, viene utilizzato l’accesso al “Sistema centralizzato per la prevenzione del furto d'identità” denominato SCIPAFI.

Persona Giuridica: per verificare esistenza, denominazione, identificativo di registrazione e sede dell’ente, il RAO può consultare il registro delle imprese dello Stato di registrazione (per gli enti italiani, il Registro delle Imprese; per gli altri Stati membri UE, il rispettivo registro delle imprese)..

Pubbliche amministrazioni, gestori di pubblici servizi e società a controllo pubblico: per gli enti italiani di questa categoria il RAO consulta l’Indice dei domicili digitali delle pubbliche amministrazioni (IPA, art. 6-ter D.Lgs. 82/2005) e verifica esistenza, denominazione, codice fiscale, sede e, ove riportato, il responsabile dell’ente.

Carica e poteri del Sottoscrittore: il RAO li verifica sul documento allegato (§3.3.2) e, ove la carica sia riportata dal registro consultato, la confronta con i dati del registro.

3.4.6.2 Procedura tecnica di validazione

L’accesso ai registri fiduciari avviene mediante canali sicuri e controlli automatici di coerenza dei dati acquisiti.

In particolare:

- Autenticazione della fonte: la connessione verso i registri avviene tramite canali sicuri (protocollo TLS aggiornato) con autenticazione del servizio IPSP presso il fornitore del dato;
- Integrità del dato: il sistema verifica l'integrità e l'autenticità delle risposte ricevute tramite validazione dei certificati dei server della fonte;
- Corrispondenza degli attributi: gli attributi estratti dai registri vengono confrontati automaticamente con i dati forniti dal Richiedente o acquisiti dalle altre evidenze raccolte durante il processo di identificazione.

3.4.6.3 Gestione delle discrepanze

Per le differenze di codifica e per quelle sui nomi si applicano i §3.4.6.4 e §3.4.6.5.

In caso di divergenza tra i dati acquisiti da fonti autorevoli mediante OCR tramite XPressID, in conformità allo standard ICAO 9303, e i dati forniti o successivamente corretti dal Richiedente, l'operatore RAO procede alla valutazione della discrepanza sulla base degli esiti e degli score restituiti da XPressID.

Ai fini della valutazione, il RAO applica i seguenti criteri:

- Prevalenza della fonte ufficiale: i dati acquisiti dalla fonte ufficiale, ove correttamente rilevati e coerenti con il documento di identità presentato, prevalgono sui dati autodichiarati dal Richiedente. Eventuali modifiche apportate ai dati acquisiti automaticamente devono essere adeguatamente valutate dal RAO e possono comportare la correzione del dato ovvero l'invalidazione dell'esito del riconoscimento.
- Attributi critici ai fini dell'Extended Level of Identity Proofing: qualora la discrepanza riguardi uno o più attributi rilevanti ai fini del mantenimento dell'Extended Level of Identity Proofing, il processo di identificazione non viene concluso sulla base del solo esito automatizzato. Il RAO procede a una revisione manuale della discrepanza oppure, qualora non sia possibile accertare con sufficiente affidabilità la correttezza del dato, conclude il processo con esito negativo.

Nel caso di identificazione effettuata in presenza, al fine di garantire l'indipendenza della verifica e mitigare il rischio di coercizione o di indebita influenza sul Richiedente, qualsiasi modifica o correzione dei dati effettuata dal RAO è sottoposta alla validazione di un secondo operatore RAO di Intesi Group avente ruolo di Master RAO.

La validazione da parte del Master RAO costituisce un controllo indipendente sull'intervento effettuato dal RAO e deve essere completata prima della conclusione del processo di identificazione.

3.4.6.4 Gestione delle differenze di codifica degli attributi di identità

Si ha una differenza di codifica quando lo stesso attributo di identità è rappresentato in modo diverso tra le evidenze (es. zona visiva e MRZ del documento, documento e tessera sanitaria, documento e asserzione eID) o tra un'evidenza e i dati dichiarati dal Richiedente, per effetto di alfabeti diversi, segni diacritici, caratteri nazionali, separatori o formato delle date.

Per i documenti dotati di MRZ, il componente di acquisizione confronta i dati della zona visiva con quelli della MRZ, che utilizza soltanto caratteri latini non accentati, e riconosce come equivalenti le differenze dovute alle regole di compilazione e traslitterazione definite da ICAO Doc 9303 (es. Ü → UE, À → A, rimozione di apostrofi e trattini, simbolo "<", formato delle date). Per i passaporti con zona visiva in alfabeto non latino la corrispondenza avviene con la trasposizione prevista da ICAO Doc 9303. Le carte d'identità sono accettate solo con zona visiva in alfabeto latino. Una differenza sul numero del documento o sulla data di nascita non è mai considerata equivalente.

Se il controllo restituisce un avviso o un esito di non coerenza, la pratica è valutata dal RAO. Se non è possibile accertare con sufficiente affidabilità il dato, il processo si conclude con esito negativo. Nell'identificazione in presenza ogni correzione effettuata dal RAO è validata da un Master RAO (§3.4.6.3).

3.4.6.5 Gestione delle differenze negli attributi del nome

Si ha una differenza negli attributi del nome quando nome o cognome non coincidono tra le evidenze (es. documento di identità, tessera sanitaria, asserzione eID, visura camerale) o tra un'evidenza e i dati dichiarati dal Richiedente, per effetto di nomi mancanti o aggiuntivi (es. secondo nome), uso di iniziali, troncamento per limiti di lunghezza, prefissi o suffissi (es. Dr, Jr), oppure di un cambio di nome o cognome non riportato in una delle evidenze.

Il confronto tollera gli errori di lettura OCR e le differenze di spaziatura. Il nome troncato nella MRZ per limiti di lunghezza è riconosciuto come equivalente quando coincide con la parte iniziale del nome completo riportato nella zona visiva.

Le altre differenze sono valutate dal RAO. I dati riportati nel documento di identità prevalgono sui dati dichiarati dal Richiedente (§3.4.6.3). Il RAO accetta la differenza solo se è riconducibile a uno

dei casi sopra elencati e il nome riportato nel documento di identità corrisponde a quello dichiarato. Il cambio di nome o cognome non riportato nel documento è accettato solo se risulta da un'evidenza ufficiale; in caso contrario, o se non è possibile accertare con sufficiente affidabilità il dato, il processo si conclude con esito negativo. Nell'identificazione in presenza ogni correzione effettuata dal RAO è validata da un Master RAO (§3.4.6.3).

L'esito dei controlli automatici e manuali e gli operatori coinvolti sono registrati e conservati con le evidenze della sessione (§3.6.2, §4.6.2).

3.4.7 Validazione tramite Proof of Access dei recapiti

In conformità ai requisiti della norma ETSI TS 119 461 (clausola 8.3.7), Intesi Group applica una procedura di proof of access finalizzata a verificare che il Richiedente abbia il controllo esclusivo dei mezzi di comunicazione dichiarati durante il processo di identificazione.

La validazione dei recapiti costituisce una evidenza supplementare a supporto del processo di identity proofing e non è utilizzata come unica prova ai fini del raggiungimento dell'Extended Level of Identity Proofing.

3.4.7.1 Ambito di applicazione

La procedura di *proof of access* è utilizzata per la validazione dei seguenti attributi di contatto:

- numero di telefono cellulare, mediante invio di codice OTP (One-Time Password) via SMS;
- indirizzo e-mail, mediante invio di codice OTP.

L'utilizzo di tali verifiche è limitato ai casi d'uso in cui i recapiti costituiscono attributi necessari al completamento del processo di identificazione o alla gestione operativa del servizio.

3.4.7.2 Procedura di validazione

La procedura di *proof of access* prevede l'esecuzione automatizzata delle seguenti verifiche:

- Generazione della challenge: il sistema genera un codice casuale univoco con validità temporale limitata;

- Dimostrazione del possesso del recapito: il Richiedente dimostra il controllo del mezzo di comunicazione inserendo correttamente il codice ricevuto oppure selezionando il link di verifica univoco;
- Convalida della risposta: il sistema verifica la corrispondenza tra il codice generato e la risposta fornita dal Richiedente. Solo in caso di corrispondenza positiva il recapito viene considerato validato.

3.4.7.3 Limitazioni di utilizzo

La procedura di proof of access è utilizzata esclusivamente per la validazione dei recapiti di contatto dichiarati dal Richiedente.

Non vengono utilizzati meccanismi di proof of access relativi a conti bancari o ad altre risorse finanziarie come evidenze del processo di identity proofing.

3.4.8 Sistema tecnologico di acquisizione delle evidenze e controlli automatizzati

Intesi Group utilizza un sistema tecnologico integrato (XPressID VeriDas) per l'acquisizione controllata delle evidenze biometriche e documentali e per l'esecuzione di controlli automatizzati sull'autenticità e sull'integrità dei documenti di identità presentati durante i processi di identificazione.

Il sistema è impiegato come componente del processo di identity validation nei casi d'uso che prevedono:

- acquisizione guidata dell'immagine del volto del Richiedente (selfie);
- acquisizione di flussi video in tempo reale durante sessioni di identificazione remota;
- acquisizione e analisi delle immagini del documento di identità;
- verifica automatizzata delle caratteristiche fisiche e logiche del documento presentato.

Nello specifico, i casi d'uso in cui viene utilizzato sono:

- identificazione in presenza (par. 3.1.1)
- identificazione remota tramite sessione video (par. 3.1.2)

3.4.8.1 Soluzione tecnologica

La piattaforma documentale denominata XpressID, erogata in modalità Software as a Service (SaaS), fornita da Veridas Digital Authentication Solutions, S.L. consente:

- l'estrazione automatica dei dati tramite OCR e MRZ parsing;
- la verifica della coerenza strutturale del documento e delle caratteristiche di sicurezza visibili e logiche;
- l'identificazione di anomalie compatibili con tentativi di falsificazione;
- l'acquisizione guidata di immagini statiche (selfie) e flussi video in tempo reale per l'analisi biometrica del volto;
- la cattura sincronizzata di volto e documento, garantendo il legame indissolubile tra il soggetto e la prova presentata durante la sessione

La piattaforma supporta l'analisi di documenti d'identità provenienti da un ampio numero di giurisdizioni internazionali.

Le tecnologie utilizzate includono modelli di Machine Learning e Deep Neural Networks finalizzati al riconoscimento documentale e alla classificazione delle caratteristiche di sicurezza.

3.4.8.2 Controlli della sessione di acquisizione remota

Durante la sessione di identificazione remota il sistema applica controlli automatici sui parametri di acquisizione al fine di garantire qualità sufficiente delle evidenze raccolte.

Durante la sessione vengono eseguiti controlli automatici in tempo reale relativi a:

- illuminazione del volto
- nitidezza dell'immagine
- stabilità dell'inquadratura
- leggibilità del documento

Per consentire all'operatore RAO l'identificazione. Nel caso in cui i parametri risultino inferiori alle soglie configurate:

- la sessione può essere sospesa oppure
- la sessione può essere ripetuta

prima della prosecuzione del processo di identificazione.

3.4.8.3 Meccanismi di rilevamento PAD e IAD (TS 18099)

Il sistema di acquisizione biometrica utilizzato da Intesi Group integra meccanismi di rilevamento automatico delle principali classi di attacco biometriche durante le sessioni di identificazione remota.

Tali meccanismi sono applicati nell'ambito del processo di **identity validation** nei casi d'uso che prevedono acquisizione video del volto del Richiedente (par. 3.1.2).

Nelo specifico, le misure adottate sono le seguenti:

Presentation Attack Detection (PAD)

Il sistema integra controlli di Presentation Attack Detection (PAD) conformi allo standard ISO/IEC 30107 finalizzati alla rilevazione di tentativi di impersonificazione basati su:

- fotografie stampate;
- immagini visualizzate su schermo;
- riproduzioni video;
- maschere o artefatti tridimensionali.

I controlli PAD includono verifiche automatiche di liveness detection basate sull'analisi dinamica del volto acquisito durante la sessione.

Injection Attack Detection (IAD)

Il sistema integra controlli di **Injection Attack Detection (IAD)** finalizzati alla rilevazione di tentativi di alterazione del flusso video acquisito tramite:

- iniezione di stream sintetici
- utilizzo di flussi preregistrati
- manipolazioni software del dispositivo
- tecniche riconducibili a scenari di spoofing digitale (es. deepfake)

Tali controlli contribuiscono a garantire che le evidenze biometriche utilizzate nel processo di identificazione siano acquisite in tempo reale dal dispositivo del Richiedente.

Integrità della cattura e protezione contro virtual camera injection

Il sistema applica controlli tecnici finalizzati a verificare l'origine del flusso video acquisito, con l'obiettivo di ridurre il rischio di utilizzo di:

- virtual camera;
- emulatori video;
- pipeline di acquisizione alterate.

Tali controlli, nell'ambito del processo di identificazione remota, contribuiscono a garantire la coerenza tra:

- dispositivo utilizzato;
- sessione di acquisizione;
- evidenze biometriche raccolte.

Allineamento ai requisiti ETSI TS 18099

Per i processi di identificazione remota che richiedono livello Extended LoIP, i meccanismi PAD e IAD adottati sono progettati in coerenza con i requisiti dello standard TS 18099.

L'efficacia dei controlli implementati è oggetto di monitoraggio periodico nell'ambito dei processi interni di gestione della sicurezza del servizio di identity proofing.

Intesi Group definisce i seguenti obiettivi di qualità per i processi automatizzati, in linea con gli obiettivi definiti da XPressID:

- Biometria (FAR/FRR): Il sistema imposta come obiettivo prestazionale un **FMR (FAR)** ≤ 1×10^{-5} e un **FNMR (FRR) target** ≤ 0,003 **per la verifica facciale** (in linea con le misurazioni empiriche NIST FRTE 1:1 di Aprile 2025 che attestano un FNMR pari a **0,0027** a FMR = 1×10^{-5} per la categoria Mugshot), garantendo la massima affidabilità nel processo di identificazione e la coerenza con la documentazione tecnica di servizio.

- Antifrode (APCER/BPCER): Per il modulo PAD, l'obiettivo è maxAPCER < 1% per la liveness attiva e maxAPCER < 2% per la liveness passiva, con un BPCER target del 5%. Tali target sono monitorati ogni due anni tramite test di laboratori accreditati (ISO/IEC 19989-3 e TS 18099)

Intesi Group si impegna a verificare, tramite acquisizione di documentazione o appositi audit, che i fornitori del motore biometrico (e.g. VeriDas) testino i loro algoritmi su dataset di riferimento e aggiornati.

Trasmissione sicura delle evidenze biometriche

Le evidenze biometriche raccolte durante la sessione di identificazione remota sono trasmesse verso l'ambiente di validazione del QTSP, dal punto di acquisizione fino ai sistemi di validazione del servizio di identity proofing, attraverso canali di comunicazione cifrati basati su protocolli TLS.

3.4.8.4 Aggiornamento dei modelli documentali e dei meccanismi di rilevazione

Il fornitore mantiene aggiornati i modelli documentali, i dataset di riconoscimento e gli algoritmi di analisi antifrode al fine di includere nuovi formati documentali, recepire modifiche ai documenti esistenti e mitigare tecniche emergenti di contraffazione.

Gli aggiornamenti includono componenti di document recognition, image integrity analysis e attack detection, tenendo conto, ove applicabile, delle informazioni disponibili tramite fonti pubbliche autorevoli quali:

- PRADO;
- report ENISA;
- dataset antifrode di riferimento del settore.

3.4.8.5 Aggiornamento dei meccanismi PAD e IAD

La piattaforma include meccanismi automatici di Presentation Attack Detection (PAD) e Image Attack Detection (IAD) finalizzati alla rilevazione di:

- immagini riutilizzate
- riproduzioni fotografiche
- manipolazioni digitali
- tentativi di spoofing documentale

Tali meccanismi sono aggiornati dal fornitore sulla base dell'evoluzione delle tecniche di attacco note. dell'analisi delle vulnerabilità emergenti e delle attività di threat intelligence disponibili.

3.4.8.6 Gestione degli aggiornamenti software e monitoraggio prestazionale

Intesi Group monitora l'evoluzione della piattaforma utilizzata e integra gli aggiornamenti software rilevanti secondo il proprio processo di gestione delle componenti critiche del servizio di identity proofing.

In particolare:

- gli aggiornamenti di sicurezza sono applicati secondo le policy interne di gestione delle vulnerabilità
- gli aggiornamenti funzionali rilevanti sono valutati rispetto all'impatto sul processo di identificazione
- le prestazioni del sistema sono riesaminate periodicamente

Il riesame complessivo dell'efficacia della soluzione di validazione documentale è effettuato almeno con frequenza annuale o in presenza di modifiche significative del panorama delle minacce.

3.5 Binding al Richiedente

Questa fase ha lo scopo di verificare che il Richiedente sia il legittimo proprietario delle prove di identità presentate e che tali prove siano in suo possesso al momento dell'identificazione.

Il servizio assicura che il processo di acquisizione del volto (selfie e video) avvenga in tempo reale, valutando in modo continuo la qualità delle immagini (illuminazione, riflessi, nitidezza), rifiutando sessioni che non permettano un confronto affidabile.

In funzione della tipologia di identificazione, il processo di binding viene eseguito con modalità differenti.

3.5.1 Binding nella identificazione in presenza (Caso d'uso 3.1.1)

In questo scenario, il legame fra l'identità e il Richiedente è stabilito mediante verifica presidiata da parte del Registration Officer. Ad effettuare la verifica della corrispondenza fra il Richiedente fisicamente presente e il documento di identità presentato è un Registration Officer appositamente formato su:

- tecniche di riconoscimento di documenti falsi o alterati;

- protezione dei dati personali;
- rilevamento di tentativi di impersonificazione e attacchi.

Il Registration Officer è supportato dall'esito della verifica biometrica effettuata tramite lo strumento XPressID.

3.5.2 Binding nella identificazione da remoto (Caso d'uso 3.1.2)

In assenza di presenza fisica, il processo si basa su tecnologie biometriche e controlli automatizzati ad elevato livello di affidabilità.

Per la verifica della vitalità del soggetto, viene acquisito un flusso video in tempo reale (minimo 1280x720 pixel e 25 fps).

Il confronto Biometrico è automatizzato: un algoritmo di intelligenza artificiale confronta il volto rilevato nel video con la fotografia estratta dal documento, nel rispetto di soglie predefinite di FAR (False Acceptance Rate) e FRR (False Rejection Rate).

Gli esiti del binding automatizzato sono sottoposti alla verifica di un operatore RAO di back-office che, sulla base delle informazioni acquisite, può confermare o rifiutare il riconoscimento prima del rilascio definitivo del risultato.

3.5.3 Binding tramite eID notificati (Caso d'uso 3.1.3)

Il legame tra Richiedente e identità elettronica viene garantito dalla verifica dell'asserzione di identittà rilasciata dall'Identity Provider:

- l'autenticazione forte presso l'IdP certifica la proprietà delle credenziali;
- i dati personali contenuti nell'asserzione sono correlati ai dati inseriti nella richiesta;
- l'asserzione viene verificata automaticamente per integrità, autenticità e livello di garanzia (eIDAS High).

Nel caso di utilizzo dell'EUDI Wallet, viene verificata:

1. l'autenticità dell'emittente (Issuer) verificando che la chiave di firma appartenga a un *PID Provider* autorizzato dallo Stato Membro e presente nella Trusted Lists (EUTL).

2. l'integrità dei dati attraverso algoritmi crittografici per assicurare che i dati all'interno del PID (nome, cognome, data di nascita, codice fiscale) non siano stati modificati o manipolati dopo l'emissione.
3. lo stato di validità (Revoca) interrogando in tempo reale (o tramite liste firmate aggiornate) il servizio di revoca del PID Provider per accertarsi che quel PID specifico non sia stato sospeso, revocato o che non sia scaduto.
4. la prova che chi sta presentando il PID sia il reale proprietario del dispositivo (Holder Binding).

3.5.4 Binding Persona Giuridica (Caso d'uso 3.1.4)

Il binding è positivo solo se sono positivi: l'identificazione del Richiedente (§3.4.4), la sua corrispondenza con il modulo e la verifica della documentazione fornita (§3.4.3).

3.5.5 Binding Persona Fisica rappresentante Persona Giuridica (Caso d'uso 3.1.5)

Il binding è positivo solo se sono positivi: l'identificazione del Richiedente (§3.4.4), la sua corrispondenza con il modulo e la verifica della documentazione fornita (§3.4.3).

3.5.6 Gestione delle discrepanze

Per i casi di identificazione in presenza e identificazione da remoto, qualora il confronto automatico e quello manuale producano esiti discordanti, il processo viene sottoposto alla validazione del Master RAO.

3.5.7 Confronto del volto da parte del Registration Officer

Nei casi d'uso 3.1.1 e 3.1.2 il Registration Officer confronta il volto riportato nel documento di identità con l'aspetto del Richiedente, dal vivo o dal video e dalle immagini acquisite (§3.3.3.1), tenendo conto degli esiti del confronto biometrico automatico prodotti dal sistema XPressID. Gli esiti automatici sono di supporto e non sostituiscono la valutazione del RAO, che esegue un'analisi morfologica secondo la seguente lista di caratteristiche:

- forma generale del volto;
- fronte e attaccatura dei capelli;
- sopracciglia;
- occhi (forma, distanza, palpebre);
- naso;

- bocca e labbra;
- orecchie, se visibili;
- guance e pieghe del viso;
- segni distintivi (nei, cicatrici, tatuaggi visibili).

Il RAO valuta separatamente le caratteristiche stabili e quelle modificabili (acconciatura, barba, occhiali, trucco) e tiene conto della differenza di età tra la fotografia del documento e il Richiedente.

L'esito del confronto può essere: corrispondenza, non corrispondenza, oppure non determinabile. Il RAO conferma il binding solo in caso di corrispondenza; negli altri casi, o se la qualità dell'immagine o del video non permette un confronto affidabile, il processo si conclude con esito negativo. In caso di esiti discordanti tra il confronto automatico e quello manuale si applica il §3.5.6.

3.6 Rilascio del risultato

L'esito finale del processo di identificazone viene generato solo al termine di tutte le verifiche previste e nel rispetto dei criteri di affidabilità e sicurezza definiti dal servizio.

Questa fase conclude il processo di verifica, formalizzando l'esito e garantendo la conservazione sicura delle prove per finalità legali e di audit.

3.6.1 Tipologia di esito

Gli esiti dei controlli effettuati nell'ambito del processo di identificazione tramite IG Persona vengono elaborati secondo le regole definite dal QTSP e determinano la gestione della pratica sulla base delle soglie di affidabilità configurate.

Il Livello di Garanzia dell'Identificazione (LoA) è implicitamente selezionato all'avvio della procedura di identificazione, in funzione del livello di garanzia richiesto per la specifica pratica. L'esito positivo del processo di identificazione conferma il Livello di Garanzia dell'Identificazione (LoIP) corrispondente al livello richiesto. In particolare, l'esito dell'identificazione può risultare Extended; tale esito viene memorizzato nel database e sui log.

In funzione dell'esito ottenuto, la pratica può essere conclusa positivamente, rifiutata oppure sottoposta a verifica da parte di personale autorizzato del QTSP secondo le procedure interne.

Nel caso di identificazione remota tramite sessione video (caso d'uso 3.1.2), gli esiti dei controlli automatici sono sottoposti a valutazione da parte del Registration Officer prima della conclusione della pratica.

In caso di esito negativo dell'identificazione, il Richiedente può ripetere il processo di identificazione per un massimo di tre tentativi complessivi.

Nel caso di identificazione in presenza (caso d'uso 3.1.1), gli esiti dei controlli automatici sono gestiti secondo le regole definite dal QTSP e possono determinare la chiusura positiva, il rigetto della pratica o l'attivazione di ulteriori verifiche da parte del personale Intesi Group, che è tenuto a effettuare una verifica aggiuntiva del riconoscimento. In tale scenario, il RAO può approvare il riconoscimento solo a seguito di una verifica con esito positivo da parte degli operatori Intesi Group.

Per le pratiche relative a persone giuridiche e a rappresentanti, la pratica è conclusa dal RAO, con esito positivo o negativo, solo dopo la verifica dell'identità del Richiedente (§3.4.4) e della documentazione dell'ente (§3.4.3).

3.6.2 Raccolta e conservazione delle prove

Per ogni sessione, vengono raccolte e conservate prove dettagliate che documentano l'intero processo di identity proofing. Queste includono:

- documentazione delle evidenze, indicandone l'emittente o la fonte;
- registrazioni video o immagini acquisite durante la fase di binding, se previsto dal caso d'uso e dal contesto normativo;
- Metadati di sessione come data, ora, tipo di identificazione, esito dei controlli automatici e manuali, operatori coinvolti;
- Log di sistema contenenti dettagli sulle verifiche effettuate (OCR, biometriche, autenticazione eID).

Le evidenze raccolte vengono conservate in modo da essere protette contro eventuali manomissioni. L'integrità viene verificata settimanalmente tramite processi automatici. Gli esiti di questi controlli vengono riportati sul sistema di monitoraggio di Intesi Group, in modo che, in caso di compromissioni, il personale possa essere tempestivamente avvisato e intervenire prontamente.

Il periodo di conservazione e la cancellazione sono disciplinati dal §4.6.2.

4 CONTROLLI DI GESTIONE

I controlli di gestione, operativi e fisici applicati al servizio di Identity Proofing (IPSP) sono improntati alla massima coerenza con il framework di sicurezza già certificato per i Servizi Fiduciari Qualificati di Intesi Group. Per quanto non espressamente dettagliato nel presente manuale, si applicano integralmente le procedure definite nei Practice Statements del QTSP Intesi Group [1], adottati per i Servizi Fiduciari Qualificati, in conformità ai requisiti dello standard ETSI EN 319 401 e alle normative applicabili. L'IPSP opera come componente del servizio fiduciario sotto la responsabilità del QTSP, garantendo che le attività di verifica dell'identità siano svolte in conformità all'Extended Level of Identity Proofing (Extended LoIP) per il rilascio di certificati qualificati.

4.1 Valutazione dei rischi operativi

Intesi Group esegue e aggiorna annualmente una analisi dei rischi applicata anche al servizio di Identity Proofing, nell'ambito del sistema di gestione della sicurezza adottato per i Servizi Fiduciari Qualificati.

Per quanto riguarda l'IPSP, l'analisi dei rischi integra quanto già previsto dai *Practice Statements del QTSP Intesi Group* [1], includendo scenari specifici relativi a:

- frodi d'identità, quali tentativi di contraffazione dei documenti o di impersonificazione;
- attacchi biometrici, con riferimento a presentation attacks (PAD) e injection attacks (IAD).

Poiché il servizio è progettato per soddisfare l'Extended Level of Identity Proofing (Extended LoIP), la valutazione dei rischi considera esplicitamente la capacità del sistema di contrastare avversari con elevato potenziale di attacco (*high attack potential*).

4.2 Analisi e monitoraggio delle minacce

Intesi Group implementa e mantiene una procedura documentata ed efficace per l'analisi e il monitoraggio delle minacce, al fine di garantire che il servizio di Identity Proofing sia costantemente aggiornato e protetto contro i rischi emergenti.

Tale attività si concentra in particolare sulle nuove tecniche di frode d'identità, inclusi gli attacchi di presentazione (PAD), gli attacchi di iniezione (IAD) e l'uso di contenuti generati artificialmente tramite intelligenza artificiale ("deep fake").

La procedura prevede:

- Monitoraggio di fonti autorevoli: consultazione costante di flussi informativi settoriali, inclusi i report ENISA e le pubblicazioni PRADO sulle caratteristiche di sicurezza e sui nuovi pattern di falsificazione dei documenti di identità.
- Collaborazione tecnologica: interazione con i fornitori per integrare aggiornamenti software e modelli di apprendimento automatico addestrati su dataset aggiornati per il rilevamento delle manipolazioni documentali e biometriche.
- Analisi dei dati operativi (Servizio Antifrode): analisi sistematica dei tentativi di frode rilevati internamente, integrando i flussi provenienti dal servizio antifrode proprietario, al fine di identificare tempestivamente nuovi pattern di attacco ad alto potenziale.

I risultati di questa attività alimentano l'aggiornamento periodico della valutazione dei rischi operativi e guidano la pianificazione di iniziative di formazione e riqualificazione specifica per il personale addetto alla verifica (RAO).

4.3 Controlli di sicurezza del personale

Intesi Group applica al personale coinvolto nel servizio di Identity Proofing le politiche di selezione, affidabilità, riservatezza e controllo già adottate per i Servizi Fiduciari Qualificati, così come definite nei Practice Statements del QTSP Intesi Group [1].

Per garantire l'efficacia dei processi di verifica, il personale operativo (Registration Officer – RAO) e i progettisti del servizio sono soggetti ai seguenti requisiti specifici che coprono selezione, formazione, aggiornamento e segregazione dei compiti.

4.3.1 Selezione e affidabilità

Il personale è selezionato in base a comprovata esperienza nella gestione di servizi IT critici ed è sottoposto a verifiche di affidabilità periodiche. Al momento dell'incarico, ogni addetto sottoscrive un accordo di riservatezza e riceve un mandato formale che ne definisce ruoli e responsabilità.

4.3.2 Formazione specialistica

Prima di essere abilitato alle attività operative, il personale riceve un addestramento specifico che copre obbligatoriamente:

- Normativa eIDAS e normativa italiana.
- tecniche di prevenzione delle frodi d'identità e rilevamento di documenti contraffatti o manomessi;
- riconoscimento di attacchi biometrici, inclusi presentation attacks (PAD) e injection attacks (IAD);
- gestione dei casi di identificazione di persone giuridiche e rappresentanti legali, inclusa verifica dei poteri di rappresentanza.
- metodologie di analisi morfologica del volto per il confronto tra Richiedente e documento;
- normativa sulla protezione dei dati personali (GDPR) e procedure di sicurezza dei sistemi utilizzati.

4.3.3 Aggiornamento e riqualificazione

La formazione del personale, in particolar modo del personale che effettua la validazione dei documenti fisici, è un processo continuo che viene aggiornato con cadenza almeno annuale o tempestivamente a seguito di nuove minacce identificate dall'attività di analisi e monitoraggio delle minacce (rif. par. 4.2).

4.3.4 Separazione dei ruoli

Per prevenire conflitti di interesse e garantire l'imparzialità del giudizio, i Registration Officer non possono ricoprire altri ruoli critici all'interno delle operazioni del QTSP che possano comprometterne l'indipendenza.

4.4 Sicurezza fisica e logica

Intesi Group adotta misure di protezione fisica e logica atte a garantire l'integrità, la disponibilità e la riservatezza dei processi di verifica dell'identità, in piena coerenza con i requisiti degli standard ETSI EN 319 401 e ISO/IEC 27001.

4.4.1 Sicurezza fisica

Per quanto riguarda la protezione dei locali, il controllo degli accessi, i sistemi di monitoraggio ambientale (antincendio, HVAC, alimentazione ridondante) e le misure di continuità operativa, si applicano integralmente le disposizioni definite nei Practice Statements del QTSP Intesi Group [1].

I sistemi utilizzati per il servizio di Identity Proofing sono ospitati in data center protetti, condivisi con i servizi fiduciari qualificati (es. CA e Marcatura Temporale), e soggetti agli stessi controlli di sicurezza fisica.

4.4.2 Sicurezza logica e separazione dei sistemi

Il sistema informativo che assume la decisione finale sulla validazione dell'identità è logicamente o fisicamente separato dai sistemi informativi non critici (ad es. reti corporate o ambienti di ufficio).

L'infrastruttura di rete applica controlli di sicurezza adeguati, inclusi firewall, sistemi di rilevamento/prevenzione delle intrusioni e protezioni anti-malware, secondo quanto previsto dal framework di sicurezza del QTSP.

4.4.3 Protezione delle comunicazioni e dei dati

Per garantire la sicurezza dei flussi di dati raccolti, in particolare nei casi d'uso remoti, sono adottate le seguenti misure:

- Crittografia del canale: tutte le trasmissioni di dati identificativi, immagini e flussi video tra il dispositivo del Richiedente e l'ambiente di validazione avvengono su canali cifrati mediante protocolli TLS aggiornati, garantendo autenticità, integrità e riservatezza.
- Protezione dell'acquisizione (OCR): il sistema implementa misure per impedire l'iniezione di dati clonati o preregistrati, assicurando che la lettura delle immagini avvenga in tempo reale durante la sessione di identity proofing.
- Tutti i sistemi critici sincronizzano il proprio orologio interno con il Coordinated Universal Time (UTC). La sincronizzazione è costantemente monitorata; in caso di mancato allineamento rispetto all'UTC, vengono generati appositi allarmi e notifiche verso il gruppo Operations, che provvede tempestivamente alle necessarie attività di verifica e ripristino.
- I log operativi e le evidenze sono protetti da manomissioni (tamper-proof) mediante meccanismi di firma digitale.

4.5 Gestione degli incidenti e delle vulnerabilità

Intesi Group adotta politiche e procedure per la gestione degli incidenti di sicurezza e delle vulnerabilità in conformità ai requisiti dello standard ETSI EN 319 401 e del sistema di gestione certificato ISO/IEC 27001.

Per gli aspetti generali di governance e coordinamento, si applicano le procedure definite nel Practice Statements del QTSP Intesi Group [1].

Le modalità operative di gestione degli incidenti e delle vulnerabilità sono formalizzate nel documento interno “Procedura per la Gestione degli Incidenti di Sicurezza delle Informazioni” adottato da Intesi Group nell’ambito del proprio Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), accessibile al personale autorizzato tramite il repository documentale aziendale.

Per il servizio di Identity Proofing, il framework di gestione è esteso per affrontare le minacce specifiche legate all’identità digitale.

4.5.1 Monitoraggio e rilevamento

Il sistema monitora costantemente i processi di verifica per individuare anomalie riconducibili a tentativi di frode o ad attacchi biometrici (PAD/IAD). Particolare attenzione è rivolta ai flussi video e agli esiti dei meccanismi di liveness detection.

4.5.2 Analisi delle vulnerabilità

In coerenza con l’attività di analisi e monitoraggio delle minacce (rif. par.4.2), Intesi Group valuta l’impatto di nuove vulnerabilità che potrebbero compromettere l’affidabilità dei metodi di identificazione, in particolare in presenza di attacchi ad alto potenziale (es. deepfake avanzati).

4.5.3 Obblighi di comunicazione

In conformità alla normativa applicabile, Intesi Group effettua le comunicazioni verso le autorità competenti e gli organismi di vigilanza nei casi e con le modalità previste, tenendo conto della natura e della gravità dell’incidente.

4.5.4 Comunicazione agli interessati

Qualora un incidente possa avere effetti negativi sui dati personali o sull’identità di un Richiedente, quest’ultimo viene informato senza indebito ritardo, secondo quanto previsto dalla normativa in materia di protezione dei dati personali.

4.6 Registrazione degli Audit e conservazione delle prove

Intesi Group adotta sistemi di registrazione e conservazione che garantiscono l’immodificabilità, la riservatezza e la reperibilità di tutti gli eventi rilevanti relativi al servizio di Identity Proofing (IPSP).

Per le politiche generali di logging, protezione dei registri e gestione degli audit, si applicano le disposizioni previste nel TSP Practice Statement del QTSP Intesi Group [1], in coerenza con i requisiti ETSI EN 319 401 e ISO/IEC 27001.

4.6.1 Tipologia di eventi e evidenze raccolte

Per ogni sessione di identificazione, vengono conservate prove complete che documentano l'intero processo.

4.6.1.1 Documentazione delle evidenze

Dati estratti dal documento di identità, asserzioni eID, documentazione probatoria relativa a persone giuridiche e rappresentanti legali.

4.6.1.2 Identificativi univoci della sessione

Tracciati decisionali, esiti dei controlli biometrici (PAD/IAD), confronto facciale (face matching), eventuali alert o score di warning/KO.

4.6.1.3 Registrazioni multimediali

Immagini e flussi video acquisiti durante la raccolta dati e il binding, se previsti dal contesto normativo e dal caso d'uso.

4.6.1.4 Tracciamento operatori

Informazioni sul personale RAO o back-office coinvolto nella verifica e approvazione del processo.

Queste evidenze costituiscono prova a fini di audit, ricostruzione degli eventi e responsabilità operativa.

4.6.2 Periodo di conservazione

In conformità al DPCM 22 febbraio 2013, ai requisiti eIDAS e alle esigenze di audit, Intesi Group conserva le evidenze del processo di identificazione per 20 anni dall'emissione del certificato emesso a seguito dell'identificazione, in conformità al DPCM 22 febbraio 2013, ai requisiti eIDAS e alle esigenze di audit. A termine del periodo i dati saranno cancellati.

Se l'identificazione non porta all'emissione di un certificato, i documenti e le evidenze raccolti nel processo vengono cancellati entro una settimana dalla chiusura o dall'abbandono della richiesta. Viene conservata la richiesta di registrazione, a documentazione del processo e dell'esito.

4.6.3 Sicurezza e Integrità

Il sistema di archiviazione dei log e delle evidenze è soggetto a controlli automatici di coerenza e integrità che garantiscono l'immutabilità dei dati conservati.

Eventuali anomalie o incongruenze generano allarmi sui sistemi di monitoraggio di sicurezza.

L'accesso ai log e alle prove è consentito esclusivamente a personale autorizzato di Intesi Group, limitatamente ai ruoli di amministrazione dei sistemi e di audit, nel rispetto dei principi di segregazione dei compiti, tracciabilità degli accessi e minimizzazione dei privilegi.

4.7 Continuità operativa e cessazione

Intesi Group garantisce la resilienza, la disponibilità e la continuità del servizio di Identity Proofing (IPSP) mediante piani formalizzati di Business Continuity e Disaster Recovery, in coerenza con il framework di sicurezza del QTSP e con i requisiti ETSI EN 319 401.

4.7.1 Piani di Continuità Operativa e Disaster Recovery

Le procedure di ripristino sono progettate per ridurre al minimo l'impatto di eventi avversi quali guasti hardware, indisponibilità di sistemi, corruzione dei dati o disastri naturali.

È garantito l'allineamento costante tra sito primario e sito secondario (Disaster Recovery), al fine di preservare l'integrità delle evidenze e la continuità del servizio.

I piani di continuità e ripristino sono documentati, mantenuti aggiornati e sottoposti a test periodici almeno annuali, con registrazione degli esiti e delle eventuali azioni correttive.

4.7.2 Terminazione del Servizio

In caso di terminazione verrà applicata la procedura di cessazione definita come procedura interna. Tale procedura è rivista annualmente da un Conformity Assessment Body (CAB) ed è approvata dall'organismo di vigilanza italiano AgID.

4.8 Gestione dei fornitori (Supply-chain)

In conformità ai requisiti e in coerenza con le politiche di gestione degli approvvigionamenti del QTSP, Intesi Group seleziona, valuta e monitora i propri partner tecnologici sulla base di rigorosi criteri di sicurezza, affidabilità e conformità normativa.

Per i componenti critici del servizio IPSP relativi alla raccolta dei dati, all'estrazione OCR e alla validazione biometrica (liveness detection e face matching), Intesi Group si avvale di fornitori qualificati che hanno ottenuto certificazioni di conformità agli standard ETSI TS 119 461 ed ETSI EN 319 401.

Intesi Group impone ai propri fornitori critici l'obbligo di propagare i medesimi requisiti di sicurezza, privacy e operativi ai propri sub-fornitori (supply chain propagation), assicurando che non vi siano degradazioni nel livello di fiducia lungo la catena di fornitura.

4.8.1 Responsabilità

Intesi Group mantiene la piena responsabilità del servizio IPSP e del rispetto delle politiche di sicurezza delle informazioni e di protezione dei dati personali, assicurando che i fornitori operino in conformità al GDPR e ai requisiti tecnici e organizzativi definiti nel presente manuale.

4.8.2 Valutazione e Monitoraggio

I fornitori critici sono soggetti a una valutazione preventiva del rischio e a un monitoraggio periodico delle prestazioni, della sicurezza e della conformità, al fine di garantire il mantenimento del livello Extended LoIP e la resilienza della supply chain.

4.8.3 Accordi Contrattuali

I rapporti con i partner tecnologici sono disciplinati da accordi che impongono l'adozione di misure di sicurezza fisica, logica e organizzativa equivalenti a quelle adottate dal QTSP, incluse clausole su riservatezza, auditabilità e gestione degli incidenti.

5 CONDIZIONI GENERALI DI SERVIZIO

5.1 Tariffe del servizio

Le condizioni economiche del servizio di Identity Proofing sono definite dall'area commerciale di Intesi Group e negoziate con i clienti enterprise in specifici accordi contrattuali.

5.2 Responsabilità finanziaria e assicurazioni

Intesi Group mantiene adeguate coperture assicurative per la responsabilità civile e professionale in relazione all'erogazione dei servizi fiduciari e dei servizi di Identity Proofing, in coerenza con quanto previsto dalle proprie politiche aziendali e dai requisiti normativi applicabili al QTSP.

5.3 Privacy e protezione dei dati personali

Il trattamento dei dati personali avviene nel rispetto del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale applicabile.

- I dati raccolti sono limitati a quanto strettamente necessario per l'esecuzione del processo di Identity Proofing.
- I dati biometrici sono trattati nel rispetto delle basi giuridiche previste dalla normativa applicabile e delle misure di sicurezza rafforzate previste per categorie particolari di dati.
- I tempi di conservazione sono definiti in funzione delle finalità del servizio e degli obblighi normativi e di audit.

Intesi Group ha condotto adeguate valutazioni in ambito privacy per il servizio di identity proofing.

5.4 Diritti di proprietà intellettuale

Il presente manuale e i processi tecnici descritti sono di proprietà di Intesi Group S.p.A. I Richiedenti conservano la titolarità dei propri dati personali e degli eventuali segni distintivi utilizzati nel contesto del servizio.

5.5 Limiti di responsabilità

Intesi Group non risponde di danni derivanti da uso improprio del servizio o da informazioni false fornite dal Richiedente. La responsabilità del QTSP è disciplinata dai termini contrattuali applicabili al servizio di riferimento.

5.6 Reclami, risoluzione delle dispute e legge applicabile

Le modalità di gestione dei reclami e delle controversie sono disciplinate nelle “Condizioni Generali di contratto del servizio di certificazione” e nei documenti contrattuali applicabili.

I sottoscrittori e i richiedenti i certificati sono invitati a fare riferimento al Capitolo 11 delle “Condizioni Generali di contratto del servizio di certificazione” e/o alle “Condizioni Generali di contratto del servizio di marcatura temporale”, pubblicate sul sito istituzionale di Intesi Group.

Tutti i clienti o le terze parti possono presentare reclami o inviare segnalazioni scrivendo una email, preferibilmente PEC, all'indirizzo tsp@ig-trustmail.com.

L'e-mail dovrà contenere i dati identificativi del mittente (nome, cognome, indirizzo e codice fiscale o partita IVA) e una descrizione dettagliata delle motivazioni alla base del reclamo o della segnalazione.