Namirial Onboarding
Manuale Operativo
Practice Statement per il servizio di identificazione da remoto

Categoria	**Manuale Operativo**	Codice documento	**NAM-NOB-MO**	**Namirial S.p.A.**
Redatto da	**Noemi Cardinaletti**	Classificazione	**Documento pubblico**	**Il Legale Rappresentante**
Verificato da	**Libero Rignanese**	Versione	**1.3**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**08/06/2026**	--

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 10-06-2026 16:15:47
IP address: 185.5.246.18

CERTIFIED ISO 9001

CERTIFIED ISO/IEC 27001

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italy | Tel. +39 071 63494 | www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426 C.F. and registration at Ancona Companies Reg. N. 02046570426 | REA N. AN – 157295 Addressee code T04ZHR3 | Share capital € 8,256,361.60 fully paidaid-up Company subject to the management and coordination of Ink (BC) Holdco Spa – Tax Code 14254460968

INDICE

Storia delle modifiche

Versione	Data	Motivatione	Modifica
1.3	08.06.2026	Aggiornamento	Revisione dei parr. 9 e 12; Introduzione di un framework articolato su due modelli operativi (Partner QTSP / Partner non-QTSP).
1.2	29.10.2025	Aggiornamento	Aggiunta di nuovo flusso di onboarding (§ 4.3.1); Aggiunta del rilevamento attivo della vitalità (§ 4.3.1)
1.1	15.09.2025	Prima emissione del documento	Versione consolidate e completa di informazioni tecniche
1.0	28.08.2025	Prima bozza	

Riferimenti tecnici e normativi

Nell'erogazione del servizio, Namirial S.p.A. si conforma alle norme e ai regolamenti europei e nazionali applicabili. I principali riferimenti normativi sono riportati nella tabella seguente.

NORMATIVA	DESCRIZIONE
eIDAS 910/2014	Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
eIDAS 1183/2024	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 a un'identità digitale
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
GDPR (EU) 2016/679	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
ICAO Doc 9303 pt.3	Machine Readable Travel DocumentsPart 3: Specifications Common to all MRTDs
ICAO Doc 9303 pt.4	Machine Readable Travel Documents: Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs
ICAO Doc 9303 pt.10	Machine Readable Travel Documents: Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Figura 1: Riferimenti tecnici e normativi

Definizioni e acronimi

Di seguito sono riportati i significati degli acronimi e dei termini specifici, fatti salvi quelli di uso comune.

Termine o Acronimo	Significato
AgID [Agenzia per l'Italia Digitale]	Agenzia per l'Italia Digitale. Ente governativo italiano responsabile della promozione dell'innovazione digitale e della definizione delle regole tecniche per i sistemi informativi della pubblica amministrazione.
APCER [Attack Presentation Classification Error Rate]	tasso di errore con cui il sistema accetta erroneamente una presentazione di attacco come se fosse genuina.
Attributo	informazione strutturata associata a un soggetto, oggetto o servizio, utilizzata per descriverne caratteristiche, proprietà, ruoli o condizioni operative nell'ambito del servizio fiduciario.
Audit trail	documento contenente l'insieme delle registrazioni cronologiche che documentano tutte le operazioni di verifica dell'identità.
Autenticazione	procedura finalizzata alla verifica dell'identità o dell'autenticità di un soggetto, dispositivo o processo, quale prerequisito per l'accesso a sistemi, dati o servizi fiduciari.
AVA Valutazione avanzata della vulnerabilità	valutazione della vulnerabilità che misura la resistenza di un prodotto o sistema a potenziali attacchi.
BAC [Basic Access Control]	meccanismo di controllo degli accessi definito dalle specifiche ICAO Doc 9303, utilizzato nei documenti elettronici di viaggio per limitare l'accesso ai dati memorizzati nel chip contactless ai soli soggetti in possesso delle informazioni presenti nella zona MRZ (Machine Readable Zone) del documento.
BPCER [Bona Fide Presentation Classification Error Rate]	tasso di errore con cui il sistema rifiuta erroneamente una presentazione genuina (non di attacco).
CA [Certification Authority]	entità fidata responsabile dell'emissione, gestione, sospensione, revoca e rinnovo dei certificati digitali nell'ambito di un'infrastruttura a chiave pubblica (PKI), nonché della verifica dell'associazione tra l'identità del soggetto e la relativa chiave pubblica.
CIE [Carta di Identità Elettronica]	documento di identità elettronico emesso dallo Stato italiano, conforme agli standard europei e alle specifiche ICAO Doc 9303, dotato di microprocessore contactless contenente dati identificativi, biometrici e certificati elettronici utilizzabili ai fini dell'identificazione fisica e digitale del titolare.

Termine o Acronimo	Significato
Certificato qualificato	certificato elettronico conforme ai requisiti del Regolamento (UE) n. 910/2014 (eIDAS), rilasciato da un prestatore di servizi fiduciari qualificato (QTSP), che attesta l'identità del titolare e associa tale identità ai dati di verifica della firma elettronica, consentendo la creazione di una firma elettronica qualificata con valore legale equivalente alla firma autografa.
Documento di identità	documento emesso da un'autorità pubblica o riconosciuta, in forma cartacea o elettronica, che consente l'identificazione univoca del titolare e può essere utilizzato anche per l'autenticazione in contesti fisici e digitali.
Documento di identità digitale	documento di identità emesso in formato elettronico, dotato di elementi di sicurezza logici e/o crittografici (ad es. chip, certificati digitali o credenziali verificabili), che consente l'identificazione certa del titolare sia in contesti fisici sia in contesti digitali, anche ai fini dell'autenticazione a servizi online.
Documento di identità fisico	documento di identità emesso in forma cartacea o plastificata da un'autorità competente, che consente l'identificazione visiva e, se previsto, automatica del titolare mediante elementi di sicurezza fisici e/o machine-readable (es. MRZ, barcode, chip contactless).
Documento elettronico	documento redatto e conservato in formato digitale, consultabile e gestibile mediante sistemi informatici.
eID [Electronic Identity]	insieme di dati e credenziali elettroniche che rappresentano l'identità di un soggetto nel contesto dei servizi fiduciari e dei sistemi di identificazione elettronica, ai sensi del Regolamento (UE) eIDAS.
eIDAS	Regolamento (UE) n. 910/2014 sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno, modificato dalla Direttiva (UE) 2022/2555 e dal Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024 che modifica il Regolamento (UE) n. 910/2014 con riguardo all'istituzione del Quadro europeo per l'identità digitale, fornisce un quadro normativo per l'identificazione elettronica di persone fisiche e giuridiche e per i servizi fiduciari.
eMRTD [Electronic Machine-Readable Travel Document]	documento di viaggio elettronico conforme alle specifiche ICAO Doc 9303, dotato di chip contactless che memorizza dati anagrafici, biometrici e di sicurezza del titolare, utilizzato per l'identificazione e la verifica automatizzata dell'identità ai valichi di frontiera.
EUDI Wallet	portafoglio digitale sicuro che consente ai cittadini, ai residenti e alle imprese europee di conservare e gestire le proprie credenziali d'identità e i documenti ufficiali (ad es. patente di guida, diplomi) in forma elettronica.
Face matching	processo biometrico di confronto tra due immagini del volto al fine di verificare che appartengano alla stessa persona

Termine o Acronimo	Significato
FAR [False Acceptance Rate]	tasso di falsa accettazione: indicatore di prestazione dei sistemi biometrici che misura la probabilità che il sistema accetti erroneamente un soggetto non autorizzato o non corrispondente all'identità dichiarata.
FRR [False Rejection Rate]	tasso di falsa rigettazione: indicatore di prestazione dei sistemi biometrici che misura la probabilità che il sistema rifiuti erroneamente un soggetto legittimo, non riconoscendone l'identità corretta.
GDPR	(General Data Protection Regulation - Regolamento UE 2016/679) è la normativa fondamentale dell'Unione Europea che disciplina la protezione e il trattamento dei dati personali. Il suo scopo è restituire ai cittadini il controllo sui propri dati e uniformare la privacy all'interno dell'UE.
IAD [Injection Attack Detection]	insieme di controlli e contromisure logiche e/o hardware destinati a identificare tentativi di manipolazione del flusso dati in sistemi di identificazione elettronica o biometrica, in cui input sintetici o non provenienti dal sensore autentico vengono iniettati per eludere i meccanismi di autenticazione o acquisizione.
Identificazione elettronica	processo di utilizzo di dati di identificazione personale in forma elettronica per attestare l'identità di una persona fisica o giuridica in un sistema digitale, ai sensi del Regolamento (UE) eIDAS.
Identity proofing	processo mediante il quale viene verificata l'identità dichiarata di un soggetto attraverso l'acquisizione, la validazione e la correlazione di evidenze identificative, documentali e biometriche, al fine di stabilire un livello adeguato di affidabilità dell'identità.
IPSP [Identity Proofing Service Provider]	soggetto o entità responsabile dell'esecuzione del processo di verifica dell'identità di una persona fisica o giuridica, mediante l'uso di procedure e controlli documentali, biometrici o elettronici, al fine di stabilire con un livello di affidabilità predefinito la corrispondenza tra l'identità dichiarata e quella reale.
Liveness detection	Rilevamento della vitalità - processo volto a verificare che il soggetto sottoposto all'identificazione sia una persona fisica reale, presente e viva al momento della sessione di identificazione, contrastando tentativi di impersonificazione mediante fotografie, video preregistrati, maschere, deepfake o altri artefatti.
LoA [Level of Assurance]	livello di fiducia attribuito al processo di identificazione elettronica e ai mezzi utilizzati per verificare l'identità di un soggetto, che descrive il grado di certezza che una determinata identità sia correttamente stabilita e gestita.

Termine o Acronimo	Significato
LoIP [Level of Identity Proofing]	livello di rigore applicato nel processo di verifica dell'identità di un soggetto, che descrive l'intensità e la profondità dei controlli effettuati per stabilire la corrispondenza tra l'identità dichiarata e quella reale, in funzione del rischio e del contesto d'uso.
Marca temporale qualificata	evidenza elettronica generata da un'autorità di marcatura temporale che lega in modo affidabile un hash di dati a un riferimento temporale, garantendo prova di esistenza, integrità e non alterazione dei dati nel tempo, secondo i requisiti del regolamento (UE) eIDAS e degli standard etsi per i servizi fiduciari.
MRZ [Machine Readable Zone]	porzione standardizzata di un documento di identità o di viaggio, conforme alle specifiche ICAO doc 9303, costituita da una o più righe di caratteri ottici leggibili automaticamente, contenenti dati essenziali del titolare codificati secondo un formato predefinito per la lettura da parte di sistemi automatici.
Namirial PID	servizio o componente offerto da namirial per l'emissione, gestione e validazione del PID (person identification data) all'interno di soluzioni di identità digitale e wallet conformi al regolamento (UE) eIDAS 2, utilizzato per attestare in forma elettronica gli attributi identificativi di una persona fisica in modo verificabile e interoperabile.
NFC [Near Field Communication]	tecnologia di comunicazione wireless a corto raggio che consente lo scambio di dati tra dispositivi compatibili posti a distanza molto ravvicinata (tipicamente pochi centimetri), basata su accoppiamento elettromagnetico e utilizzata per autenticazione, identificazione e pagamento contactless.
OCR [Optical Character Recognition]	riconoscimento ottico dei caratteri: tecnologia che consente la conversione automatica di testo presente in immagini, documenti scannerizzati o supporti visivi in dati testuali digitali, rendendoli elaborabili da sistemi informatici.
OID [Object Identifier]	identificatore univoco globale e gerarchico utilizzato per denominare in modo non ambiguo oggetti, attributi, algoritmi o politiche all'interno di sistemi informativi e crittografici, in particolare in ambito PKI e standard x.509.
Onboarding	processo mediante il quale un soggetto viene registrato e abilitato all'utilizzo di un servizio, a seguito delle attività di identificazione, verifica dell'identità, acquisizione delle informazioni necessarie e accettazione delle condizioni applicabili.

Termine o Acronimo	Significato
PACE [Password Authenticated Connection Establishment]	protocollo crittografico avanzato definito nelle specifiche icao doc 9303 per stabilire un canale di comunicazione sicuro tra un lettore e il chip di un documento elettronico di viaggio, basato su autenticazione tramite password o informazioni equivalenti e progettato per sostituire o integrare il bac, offrendo un livello di sicurezza superiore contro attacchi di intercettazione e accesso non autorizzato.
PAD [Presentation Attack Detection]	insieme di tecniche e controlli utilizzati nei sistemi biometrici per rilevare e prevenire attacchi di presentazione, ossia tentativi di inganno del sensore biometrico mediante l'uso di artefatti (es. maschere, fotografie, impronte artificiali, replay o deepfake) al fine di impersonare un soggetto legittimo.
PID [Person Identification Data]	insieme strutturato di dati che rappresentano l'identità di una persona fisica, includendo attributi identificativi e informazioni associate utilizzate per l'identificazione e l'autenticazione in sistemi digitali, in particolare nell'ambito di eIDAS 2 e dei portafogli di identità digitale.
PRADO [Public Register of Authentic identity and travel Documents Online]	è una banca dati ufficiale gestita dal Consiglio dell'Unione Europea che fornisce informazioni sulle caratteristiche di sicurezza e sui formati dei documenti di viaggio e d'identità autentici rilasciati dagli Stati membri dell'UE, nonché da alcuni paesi terzi. È destinata principalmente all'uso da parte delle autorità pubbliche, degli agenti di controllo alle frontiere e di altri soggetti coinvolti nella verifica dell'identità.
QTSP [Qualified Trust Service Provider]	prestatore di servizi fiduciari qualificato che fornisce uno o più servizi fiduciari qualificati ed è stato riconosciuto come tale dall'organismo di vigilanza competente ai sensi del Regolamento (UE) n. 910/2014 (eIDAS) e delle relative disposizioni di attuazione.
Relying Party	entità che riceve e utilizza attestazioni di identità, certificati digitali o altri servizi fiduciari emessi da un provider di identità o da un'autorità di certificazione, assumendo la responsabilità di validarne la fiducia ai fini dell'autenticazione o autorizzazione.
Richiedente	persona fisica che si rivolge all'IPSP per la verifica dell'identità e il rilascio di Certificati Qualificati, la cui identità deve essere comprovata.
SPID [Sistema Pubblico di Identità Digitale]	sistema nazionale italiano di identità digitale che consente ai cittadini e alle imprese di accedere ai servizi online della pubblica amministrazione e dei soggetti privati aderenti, mediante credenziali rilasciate da identity provider accreditati e basate su diversi livelli di sicurezza e autenticazione.

Termine o Acronimo	Significato
Servizio fiduciario [Trust Service]	servizio elettronico disciplinato dal regolamento (UE) eIDAS che supporta la creazione, verifica e validazione di dati elettronici affidabili, inclusi certificati, firme e sigilli elettronici, marche temporali e servizi di recapito elettronico certificato, fornito da un prestatore qualificato o non qualificato.
VIZ [Visual Inspection Zone]	area visiva di un documento di identità o di viaggio, destinata alla lettura e verifica manuale delle informazioni stampate, incluse le generalità del titolare e gli elementi di sicurezza visibili a occhio nudo o con strumenti di ingrandimento.
WSCD [Wallet Secure Cryptographic Device]	elemento hardware con caratteristiche di sicurezza e resistenza alle manomissioni, utilizzato nei sistemi di identità digitale per eseguire operazioni crittografiche in ambiente isolato e affidabile, in particolare nell'ambito dei portafogli di identità digitale conformi a eIDAS 2.
Web Interface	interfaccia accessibile via browser per l'interazione con un sistema informatico.

Figura 2: Definizioni e acronimi

Descrizione sintetica di Namirial S.p.A.

Namirial S.p.A. è una multinazionale italiana dell'Information Technology con sede legale a Senigallia (Ancona), attiva nel settore del Digital Transaction Management (DTM). Fondata nel 2000, l'azienda sviluppa soluzioni e tecnologie per la verifica dell'identità digitale, la firma elettronica, la fatturazione elettronica e la gestione sicura dei flussi documentali digitali. Con oltre 1.000 dipendenti e sedi distribuite sul territorio nazionale e in diversi paesi europei ed extraeuropei, Namirial serve oggi una clientela che spazia da professionisti e PMI fino a grandi organizzazioni enterprise, pubbliche amministrazioni e operatori di mercati regolamentati, a cui fornisce servizi digitali ad alto valore aggiunto integrati nei rispettivi processi di business.

Namirial è Qualified Trust Service Provider (QTSP) ai sensi del Regolamento eIDAS (UE n. 910/2014) ed è iscritta nell'elenco pubblico dei prestatori di servizi fiduciari qualificati tenuto da AgID — Agenzia per l'Italia Digitale. Il portafoglio di servizi fiduciari si è consolidato nel tempo attraverso successive qualificazioni: dalla gestione della Posta Elettronica Certificata (dal 2007) e del servizio di conservazione digitale a norma (dal 2014), alla firma elettronica qualificata (dal 2010), fino all'accreditamento come Identity Provider nell'ambito del Sistema Pubblico di Identità Digitale SPID (dal 2017). A queste si affiancano oggi soluzioni avanzate di onboarding digitale e verifica dell'identità a distanza, erogate in modalità API-first a beneficio di clienti che integrano i servizi Namirial nei propri flussi operativi.

Namirial S.p.A. è:

eIDAS-compliant

Qualified Trust Service Provider eIDAS

Namirial è QTSP secondo la definizione eIDAS per i servizi:

- Emissione del certificato qualificato per la firma elettronica;
- Emissione del certificato qualificato per il sigillo elettronico;
- Emissione della marca temporale qualificata;
- Conservazione di firme qualificate e sigilli qualificati

Namirial è inserito nella lista EU Trust Services Dashboard ed è accreditata dal governo italiano come prestatore di servizi fiduciari.

AGID Agenzia per l'Italia Digitale

Prestatori di servizi fiduciari attivi in Italia

Certificato 910/2014 eIDAS – Prestatori Servizi Fiduciari Qualificati

Electronic Registered Delivery – Gestore PEC

accreditato da AgID ed autorizzato alla gestione di caselle e domini di Posta Elettronica Certificata (PEC), fornisce il servizio di Sicurezza Postale dal 2007.

Elenco gestori PEC

Il servizio è qualificato SaaS livello QC1 presso ACN e inserito nel Catalogo delle infrastrutture digitali e dei servizi cloud

Catalogo infrastrutture digitali e servizi cloud – PEC

Identificazione Elettronica – Identity Provider SPID

Namirial fornisce servizi fiduciari di identificazione digitale SPID ed è accreditata dal governo italiano secondo gli standard europei eIDAS ai sensi del:

- DPCM 24/10/2014;
- Regolamento di attuazione UE 2015/1502 della Commissione;
- Regolamento (UE) 910/2014 eIDAS, art. 24 per la prestazione di servizi fiduciari di Identificazione Digitale.

Identity provider accreditati

Certificazione ETSI EN 319 401

Long Term Archiving Provider -Soggetto Conservatore

in conformità a:

- Regole Tecniche ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale;
- Regolamento (UE) 910/2014 eIDAS, art. 24 per la prestazione di servizi fiduciari di Conservazione a Norma.

Namirial fornisce il servizio di Archiviazione a lungo termine dal 2014, è qualificata da AgID e dall'Agenzia per la cybersicurezza.

Il servizio è qualificato SaaS livello QC2 presso ACN e inserito nel Catalogo delle infrastrutture digitali e dei servizi cloud.

Conservatori Qualificati

Catalogo infrastrutture digitali e servizi cloud – NamirialArchive

Certificata UNI EN ISO 9001:2015. Namirial ha conseguito il certificato **Quality Management System** rilasciato da Bureau Veritas Italia S.p.A.

Certificata ISO/IEC 27001:2022. Namirial ha conseguito il certificato **Information Security Management System integrato dai controlli previsti dalle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019** rilasciato da Bureau Veritas Italia S.p.A.

Certificata ISO 37001:2016

Namirial ha conseguito il certificato **Anti-bribery management systems** rilasciato da Bureau Veritas Italia S.p.A.

Certificata UNI PdR 125:2022

Namirial ha conseguito il certificato **Sistema di gestione per la Parità di Genere** rilasciato da Bureau Veritas Italia S.p.A.

Certificata da Adobe. Da giugno 2013 Namirial è membro dell'AATL (Adobe Approved Trust List).

1 INTRODUZIONE

1.1 Scopo e ambito di applicazione

Il presente documento è un Manuale Operativo emesso da Namirial S.p.A. e descrive le regole e le procedure operative adottate da Namirial per l'erogazione del servizio di **Onboarding.**

Il presente documento delinea le regole e gli standard adottati dall'**Identity Proofing Service Provider** Namirial S.p.A. per l'erogazione di servizi di verifica dell'identità per persone fisiche mediante un **sistema di video-identificazione remota non presidiata**.

L'*Addendum Partner*, sottoscritto tra Namirial e ciascun Partner prima dell'attivazione di tale servizio, costituisce parte integrante del presente Manuale Operativo. Definisce tutte le disposizioni specifiche del Partner in materia di protezione dei dati, obblighi verso i richiedenti, allocazione delle responsabilità, copertura assicurativa e condizioni contrattuali.

Sono disponibili due versioni:

- l'Addendum Partner Namirial QTSP, precompilato con i dati di Namirial, applicabile qualora Namirial agisca sia come IPSP sia come QTSP;
- l'Addendum Partner Template, da completare e sottoscrivere da parte di qualsiasi altro Partner. In caso di conflitto tra il presente Manuale Operativo e un Addendum Partner sottoscritto, l'Addendum Partner prevale per le materie che disciplina.

1.2 Nome e identificativo del documento

Il presente documento, denominato "*Namirial Onboarding Manuale Operativo Practice statement per il servizio di identificazione da remoto*", con codice documento **NAM-NOB-MO** è identificato dal livello di versione e dalla data di rilascio su tutte le pagine. Il preambolo del documento include inoltre un paragrafo con la cronologia delle modifiche apportate.

Namirial esegue, almeno una volta all'anno, un audit di conformità del servizio di Onboarding e, ove necessario, aggiorna il presente documento in funzione dell'evoluzione della normativa e degli standard tecnologici.

Il presente documento e gli eventuali ulteriori documenti emessi per materie o casi specifici, come *addendum* al presente Manuale Operativo, sono pubblicati da Namirial e consultabili elettronicamente al seguente indirizzo:

https://www.namirial.com/it/documentation/

Il documento è pubblicato in formato PDF firmato per garantirne l'origine e l'integrità.

1.3 Partecipanti e responsabilità

1.3.1 Soggetti coinvolti

I soggetti menzionati nel presente documento sono:

a) **IPSP (Identity Proofing Service Provider):** Fornitore del Servizio di identificazione;
b) **Richiedente:** la persona fisica che presenta la richiesta di verifica ed esegue l'identificazione;
c) **Relying Party**, la persona fisica o giuridica che si affida al servizio di verifica dell'identità o a un servizio fiduciario;
d) **Operatori** di back-office.

1.3.1.1 Fornitore del Servizio di Identificazione

Un Fornitore del Servizio di identificazione (IPSP) è un'entità qualificata o accreditata che fornisce servizi di identificazione.

Namirial S.p.A. è un Prestatore di Servizi Fiduciari accreditato riconosciuto da un organismo di vigilanza (come AgID in Italia o a livello UE), che emette servizi digitali qualificati quali firme elettroniche qualificate e sigilli elettronici.

In questo caso, il QTSP agisce anche in qualità di IPSP, eseguendo direttamente le verifiche di identity proofing in conformità agli standard ETSI EN 319 461.

I dettagli completi dell'organizzazione che agisce in qualità di IPSP sono i seguenti:

Ragione sociale	Namirial S.p.A.
Sede legale	VIA CADUTI SUL LAVORO, 4 60019 – SENIGALLIA (AN) +39 071.63494
Partita IVA	IT02046570426
Sito web del servizio	https://www.namirial.com/it/onboarding/
Sito web	http://www.namirial.com

Figura 3: Dati identificativi Identity Proofing Service Provider

1.3.1.2 Richiedente

Persona fisica la cui identità viene sottoposta al processo di onboarding ai fini dell'emissione o dell'utilizzo di un servizio fiduciario.

1.3.1.3 Relying Party

Soggetto che fa affidamento sull'esito del processo di onboarding o sui servizi fiduciari associati, assumendo valide le informazioni di identità verificate.

1.3.1.4 Operatore di back-office

Un operatore di back-office per la verifica dell'identità è un soggetto opportunamente formato per verificare l'identità di un Richiedente, utilizzando specifiche procedure e tecnologie.

Gli operatori di back-office devono:

- essere autorizzati allo svolgimento delle operazioni di verifica delle identità da un IPSP o TSP certificato;
- operare nel rispetto delle procedure operative e dei requisiti di sicurezza definiti dal IPSP o TSP;
- garantire la riservatezza, l'integrità e la protezione dei dati personali e delle informazioni trattate durante lo svolgimento delle attività di onbaording, nel rispetto del Regolamento (UE) 2016/679 (GDPR) e della normativa applicabile in materia di protezione dei dati personali;
- verificare e trattare le evidenze di identificazione esclusivamente nell'ambito delle autorizzazioni assegnate;
- segnalare tempestivamente anomalie, incidenti di sicurezza, sospetti di frode o non conformità rilevate nel processo di identificazione;
- utilizzare piattaforme sicure per la video-identificazione in tempo reale o differita;
- mantenere adeguati livelli di formazione, competenza e aggiornamento relativamente alle procedure di verifica dell'identità e rilevamento delle frodi;

2 AMMINISTRAZIONE DEL MANUALE OPERATIVO

2.1 Pubblicazione e archiviazione

La responsabilità del presente documento è in capo alla figura con il ruolo di 'Responsabile del Servizio", che si occupa della verifica, della pubblicazione e dell'aggiornamento.
Le comunicazioni relative al presente documento possono essere inviate all'attenzione del suddetto responsabile ai seguenti indirizzi:

e-mail: infotsp@namirial.com

Poiché per il servizio oggetto del presente documento non è richiesto uno specifico Object Identifier (OID), l'OID che identifica Namirial S.p.A. è iso(1) identified-organisation(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

Il repository di Namirial è disponibile all'indirizzo:

https://www.namirial.com/en/documentation/

Il presente documento è pubblicamente disponibile e accessibile in sola lettura. Namirial gestisce l'accessibilità al repository in modo autonomo e continuo (24x7x365) ed è direttamente responsabile dello stesso.

Il presente documento viene pubblicato ogniqualvolta venga aggiornato.

3 OPERAZIONI DI ONBOARDING

Lo scopo principale dell'Onboarding da remoto è verificare l'identità della persona sottoposta al processo di identificazione per accertare che si tratti effettivamente di chi dichiara di essere e abilitarla all'utilizzo del servizio richiesto nel rispetto dei requisiti normativi, contrattuali e di sicurezza applicabili. Le soluzioni mirano a validare l'identità di persone fisiche.

La soluzione NOB è composta da moduli tecnologici che, singolarmente o in combinazione, consentono un processo di onboarding digitale sicuro conforme ai requisiti di identity proofing, sicurezza, affidabilità, tracciabilità e gestione delle evidenze previsti dallo standard ETSI TS 119 461 V2.1.1 e dal quadro normativo eIDAS applicabile. In particolare, le soluzioni garantiscono un metodo sicuro e affidabile per l'identificazione di persone fisiche in conformità ai requisiti di ETSI 119 461 e dell'Atto di Esecuzione dell'articolo 24 del Regolamento eIDAS.

Grazie ai controlli descritti nei paragrafi seguenti, sarà possibile implementare le soluzioni e i processi delineati al paragrafo 4.

3.1 Raccolta dei dati

La procedura richiede che il Richiedente utilizzi un dispositivo connesso a Internet (tablet, smartphone o PC) dotato di webcam funzionante. Un processo automatizzato guida il Richiedente attraverso un flusso di lavoro end-to-end per un'esperienza di identificazione remota non presidiata.

Ogni sessione viene avviata tramite un canale di comunicazione sicuro, garantendo riservatezza e integrità.

Prima dell'avvio della procedura di identificazione, il Richiedente deve essere preventivamente informato, in modo chiaro e comprensibile, circa lo scopo del processo di onboarding, le modalità di trattamento dei dati personali, i termini e le condizioni

applicabili al servizio nonché gli obblighi derivanti dall'utilizzo dello stesso. Il Richiedente deve inoltre prendere visione dell'informativa privacy e accettare esplicitamente i termini e le condizioni del servizio, prestando i consensi richiesti in conformità ai requisiti del processo di onboarding.

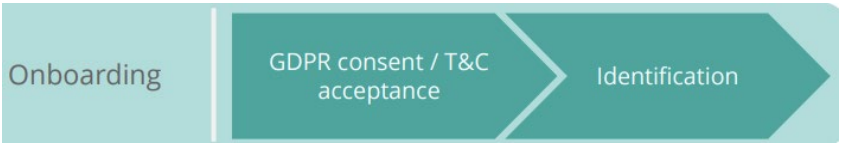

Figura 4: Flusso di avvio dell'Onboarding

Successivamente, al Richiedente viene chiesto di posizionare correttamente il documento d'identità all'interno di un apposito riquadro per consentire all'applicazione di acquisire una breve registrazione video del documento, catturando sia il fronte sia il retro. L'applicazione si asterrà dall'acquisire l'immagine qualora il documento non sia correttamente inquadrato o l'immagine non sia pienamente leggibile.

A seguito dell'acquisizione del documento, la procedura utilizza un sistema avanzato OCR per:

- estrarre i dati rilevanti dal documento di identità, inclusi nome e cognome del Richiedente, data di nascita, numero del documento e fotografia;
- estrarre I dati presenti nella zona MRZ (Machine Readable Zone).

Per determinare l'autenticità e la validità del documento di identità vengono eseguiti diversi controlli, tra cui:

- verifiche sugli elementi otticamente variabili (OVD);
- controlli del checksum della zona a lettura ottica (MRZ);
- controlli incrociati tra i dati presenti nella zona a lettura ottica (MRZ) e quelli presenti nella zona di ispezione visiva (VIZ).

L'acquisizione del documento di identità avviene esclusivamente tramite interfaccia web; non è consentito il caricamento esterno.

Al Richiedente sarà inoltre chiesto di effettuare una breve registrazione video finalizzata alla verifica della vitalità (liveness detection). La verifica della vitalità può essere eseguita mediante meccanismi attivi o passivi, in funzione della tipologia di processo di identificazione adottato.

In caso di identificazione tramite strumenti eID preesistenti, non saranno richieste azioni aggiuntive al di fuori della selezione del proprio provider eID e dell'autenticazione con il metodo supportato dal proprio eID; il sistema recupererà le informazioni sugli attributi personali e le assocerà a quelle relative al servizio richiesto (§ 3.3).

Al fine di garantire la protezione e la gestione dei dati personali in piena conformità con il Regolamento (UE) 2016/679 (GDPR), a ciascun Richiedente viene fornita in anticipo l'informativa sulla privacy.

3.1.1 Documenti di identificazione accettati

Il Richiedente può identificarsi mediante **un documento d'identità fisico o digitale valido**, nella sua forma originale.

A titolo esemplificativo, si riporta un elenco di documenti di identità ammessi, purché in corso di validità, recanti la fotografia del Richiedente e rilasciati da un'amministrazione di Stato:

- Carta d'identità,
- Passaporto,

I documenti che possono essere presentati sono reperibili nel database PRADO, al seguente link https://www.consilium.europa.eu/prado/en/prado-start-page.html.

Un documento d'identità comprende due principali categorie di informazioni:

- La Zona di Ispezione Visiva (VIZ), che riporta i dati personali del titolare del documento. Questa sezione comprende:
  - Immagine del Volto: una fotografia che rappresenta l'identità della persona.
  - Campi Dati OCR: dati testuali codificati quali nomi, cognomi, date, numeri di identificazione, numeri seriali del documento, indirizzi e informazioni analoghe.
  - Elementi di Sicurezza Fisici: protezioni fisiche integrate tra cui inchiostri otticamente variabili (OVI), microstampa, kinegram e altre caratteristiche anticontraffazione.
- La Zona di Lettura Ottica (MRZ), è l'area del documento d'identità in cui compaiono le informazioni leggibili meccanicamente. È composta generalmente da due righe (passaporto) o tre righe (carta d'identità)

In caso di documento non valido, il processo non andrà a buon fine.

3.1.2 Tipologie di dati raccolti

La presente sezione riepiloga le tipologie di dati raccolti durante i processi di onboarding e di registrazione. I dati sono classificati come **obbligatori** quando richiesti per la conformità normativa o per le funzionalità fondamentali del servizio (quali nome, cognome e codice fiscale o numero di identificazione personale), e **facoltativi** (o supplementari) quando raccolti per finalità di verifica aggiuntive.

L'insieme dei dati **obbligatori** estratti e raccolti comprende:

- Nome
- Cognome
- Numero del documento
- Paese di rilascio
- Valido dal (data)
- Valido fino al (data) – se disponibile nel documento
- Data di nascita
- Luogo di nascita
- Nazionalità
- Luogo di rilascio
- Sesso
- Codice fiscale o numero di identificazione personale

L'acquisizione dei dati identificativi avviene direttamente dalla fonte di identità utilizzata nel processo (eID o documento di identità), al fine di garantire l'accuratezza delle informazioni raccolte e ridurre il rischio di errori derivanti da trascrizione manuale. Nel caso di documenti dotati di zona a lettura ottica (MRZ), l'estrazione dei dati viene effettuata prioritariamente mediante acquisizione delle informazioni contenute nella MRZ stessa.

Qualora il processo di identificazione sia avviato da un'applicazione nativa che include il Namirial Onboarding SDK e il Richiedente fornisca documenti di identificazione digitali (conformi allo standard ICAO 9303 Parte 10 [9] con MRZ o caratteristiche analoghe), sarà possibile utilizzare l'ID NFC.

3.2 Validazione dei dati

Il processo di validazione dei dati comporta la verifica documentale delle evidenze presentate dal Richiedente, nello specifico la verifica del documento di identità

La validazione dei dati provenienti dal documento di identità costituisce una parte critica del processo complessivo di verifica. Nei casi di tentativo di frode, si verificano tipicamente due scenari comuni:

- Documenti di identità falsi, interamente contraffatti,
- Documenti di identità contraffatti, in cui documenti autentici sono stati alterati o manomessi.

Durante il processo di validazione, tutti i dati personali e le informazioni documentali fornite dal Richiedente sono sottoposti a validazione strutturata per garantire accuratezza, autenticità e affidabilità.

Il sistema effettua, automaticamente, dei controlli di coerenza logica quali:

- verifica dell'integrità del documento;
- verifica la coerenza delle informazioni acquisite su tutti i campi rilevanti, inclusi nome, data di nascita e numero del documento;
- validazione specifica sugli elementi leggibili meccanicamente, come la MRZ, inclusa la verifica del checksum.

In aggiunta, il sistema verifica l'autenticità del documento d'identità rilevando possibili segni di manomissione, verificando la coerenza tra MRZ e VIZ e analizzando specifici elementi di sicurezza (come, ad esempio, ologrammi, font ufficiali, formattazione dei bordi), includendo controlli contro attacchi di replay e tentativi di falsificazione mediante riproduzione o stampa del documento. I dati estratti dalla MRZ vengono quindi validati e confrontati con le informazioni presenti nella parte visibile del documento.

Il sistema consente inoltre di rilevare i casi in cui il medesimo documento di identità venga presentato più volte, anche qualora alcuni dati anagrafici (quali, a titolo esemplificativo, nome, cognome, data di nascita e luogo di nascita) risultino modificati o alterati rispetto alle precedenti presentazioni, mediante meccanismi di confronto e correlazione delle evidenze acquisite.

Considerato che solo i registri nazionali ufficiali o approvati a livello nazionale dovrebbero essere accettati come registri attendibili, e che la disponibilità varia da Paese a Paese, Namirial non implementa registri per la raccolta o la validazione degli attributi. Inoltre, nelle principali giurisdizioni in cui Namirial opera, tra cui Italia, Francia, Spagna, Germania e Romania, non sono disponibili al momento banche dati ufficiali o approvate a livello nazionale per la verifica automatizzata, o in tempo reale, degli attributi d'identità in condizioni compatibili con le operazioni dei servizi fiduciari. Di conseguenza, l'identificazione del Richiedente si basa sulla verifica diretta dei documenti e sulle prove autorevoli fornite dai richiedenti o da entità supervisionate.

Il processo di validazione può, a seconda dei casi d'uso, essere delegato e condotto da operatori Namirial. In tal caso, le procedure stabilite per la verifica dei documenti d'identità sono dettagliate in procedure e documentazione interna dedicata, specificatamente adattata in base al paese di emissione del documento.

Il processo si considera completato con esito positivo esclusivamente a seguito della validazione di tutti i dati richiesti. Eventuali incongruenze, anomalie o dati non verificabili comportano il rigetto del processo ovvero l'attivazione di un'escalation per ulteriori verifiche e approfondimenti istruttori.

3.3 Identificazione tramite strumenti *eID*

L'identificazione tramite strumenti eID avviene quando il Richiedente viene identificato tramite un sistema di identità digitale preesistente.

Questa modalità prevede che il Richiedente sia, pertanto, in possesso di un **mezzo di identificazione elettronica nazionale preesistente**:

Nello specifico, Namirial prevede che l'identificazione possa essere eseguita anche da strumenti che garantiscono lo stesso livello di affidabilità (livello di garanzia elevato) notificati da altri Stati membri e pubblicati dalla Commissione Europea nella Gazzetta ufficiale, in conformità con l'art. 9 del Regolamento (UE) n. 910/2014 (eIDAS) e s.m.i, consultabili al seguente link: Overview of pre-notified and notified eID schemes

L'integrazione consente ai richiedenti di accedere ai servizi online tramite credenziali già in proprio possesso, identità federate ottenute nell'ambito dei diversi programmi nazionali di identità digitale e in conformità con il Regolamento eIDAS.

Il Richiedente esegue l'autenticazione inserendo le proprie credenziali, consentendo l'acquisizione dei dati certificati e accelerando il processo di onboarding. Il sistema recupera le informazioni personali e le associa a quelle relative al servizio di sottoscrizione richiesto.

3.4 Associazione al Richiedente (*binding*)

L'associazione al Richiedente, o *binding*, viene eseguita tramite tecnologia biometrica e/o verifica manuale.

Le procedure descritte di seguito garantiscono coerenza e ripetibilità, contribuendo a evitare errori, frodi o discrepanze nella verifica dell'identità, assicurando un elevato livello di sicurezza e affidabilità. Considerato che il furto d'identità viene effettuato con tecniche sempre più sofisticate, le tecnologie implementate sono avanzate.

3.4.1 Controlli biometrici

Il sistema implementa controlli biometrici finalizzati alla verifica dell'identità del soggetto durante il processo di remote identity proofing, in conformità ai requisiti di ETSI TS 119 461 v. 2.1.1 e agli standard biometrici applicabili.
Il controllo biometrico è la fase del processo di verifica remota dell'identità non presidiata in cui i dati biometrici di un individuo, quali le caratteristiche facciali, vengono raccolti, analizzati e confrontati con dati precedentemente registrati o contenuti in un documento di identità ufficiale.

3.4.1.1 Controlli di corrispondenza biometrica (*face matching*)

In un contesto remoto, questo controllo viene tipicamente eseguito mediante strumenti digitali (come una videocamera) e **algoritmi di verifica della corrispondenza biometrica** che analizzano automaticamente le caratteristiche fisiologiche o comportamentali dell'utente provenienti dal campione biometrico acquisito durante la sessione e l'immagine di riferimento associata all'identità dichiarata.

L'algoritmo di *face matching* è implementato 1:1 e certificato ISO/IEC 19795 con le seguenti prestazioni:

- False Match Rate inferiore allo 0,1% su migliaia di confronti;
- False Non-match Rate dello 0% su migliaia di confronti riusciti.

I dati biometrici estratti dall'immagine sono sottoposti a molteplici validazioni automatizzate per confermare che il soggetto corrisponda alla fotografia acquisita.

3.4.1.2 Controlli di presenza o *liveness*

Il rilevamento della presenza reale del Richiedente, o *liveness detection*, è una tecnica di sicurezza utilizzata nella verifica biometrica volta a determinare che i dati biometrici acquisiti, come il volto, provengano da una persona reale e fisicamente presente al momento della cattura degli stessi dati, anziché da una fonte contraffatta.

La *liveness detection* può essere implementata tramite:

- **Metodo attivo – active liveness detection:** mediante l'esecuzione, da pate del Richiedente, di determinate azioni (challenge):
  - Il sistema verifica la risposta del Richiedente in tempo reale: in caso di corretta esecuzione della challenge, il sistema conclude che il soggetto è presente, reale e attivamente coinvolto nel processo di identificazione, escludendo ragionevolmente la presenza di tentativi di spoofing.
- **Metodo passivo – passive liveness detection**, che prevede l'analisi di indicatori di presenza vitale quali la texture della pelle, il movimento degli occhi o informazioni di profondità, senza richiedere alcuna interazione da parte dell'utente:
  - Al Richiedente viene chiesto di effettuare una breve registrazione video; viene acquisito un fotogramma del volto a una risoluzione idonea all'analisi automatizzata. Se tutti i parametri qualitativi (quali illuminazione, posizionamento e risoluzione) soddisfano gli standard richiesti, il sistema acquisisce automaticamente immagini statiche del Richiedente dal flusso video. I dati biometrici estratti dall'immagine sono sottoposti a molteplici validazioni automatizzate per confermare che il soggetto corrisponda alla fotografia acquisita.

Questa fase comporta l'applicazione sistematica di tecniche anti-spoofing, garantendo che i dati biometrici provengano da un soggetto in vita e non da una fonte fraudolenta,

rispondendo alla necessità di verificare la presenza reale e l'effettiva esistenza del Richiedente.

La tecnologia di tali componenti di rilevamento è implementata con **PAD (Presentation Attack Detection)** e **IAD (Injection Attack Detection)** ed è certificata 30107-3 Level 1&2 per PAD e CEN/TS 18099 high per IAD.
Per il PAD, l'APCER (tasso di errore nella classificazione degli attacchi) e il BPCER (tasso di errore nella classificazione delle presentazioni autentiche) sono rispettivamente definiti allo 0% e fino al 15%.

I componenti analizzano molteplici caratteristiche all'interno dell'immagine per individuare artefatti e incongruenze e rilevare tentativi di spoofing, quali:

- **Video Replay attack** — si verifica quando un attore malevolo registra un video in presenza fisica e tenta di riprodurlo, tramite un display esterno, posizionandolo davanti alla webcam utilizzata per l'identificazione di un Richiedente;
- **Printed Photo attack** — si verifica quando un attor malevolo registra un video o scatta fotografie e poi stampa uno o più fotogrammi su carta per presentarli, tramite display esterno, davanti alla webcam utilizzata per l'identificazione di un Richiedente;
- **3D Mask attack** — si verifica quando un attore malevolo si presenta fisicamente davanti alla webcam utilizzata per l'identificazione del Richiedente, utilizzando un artefatto fisico (come, ad esempio, una maschera in silicone o plastica) costruita per imitare i tratti del volto di un individuo;
- **Video Injection** – si verifica quando un attore malevolo, tramite l'utilizzo di specifici software, preregistra un video di un altro individuo che completa l'intero processo di identificazione per iniettarlo in tempo reale nel flusso di onboarding, simulando una sessione live;
- **Deepfake Video Injection** — si verifica quando un attore malevolo utilizza un video sintetico o manipolato tramite tecniche di intelligenza artificiale generativa, che viene immesso nel canale di acquisizione video al fine di simulare la presenza di un soggetto legittimo durante il processo di verifica biometrica., simulando una sessione live.

3.4.2 Verifica manuale

La verifica manuale nell'ambito del processo di validazione dei dati di identità, il processo viene eseguita, in back-office, da un **operatore umano esperto**, tramite il monitoraggio in tempo reale delle sessioni di onboarding, con una visione aggiornata di tutti i controlli eseguiti e delle azioni da compiere.

La soluzione si avvale di un team di esperti antifrode, garantendo esperienza e risposta rapida alle minacce emergenti. Tali risorse operano 24/7.

I controlli consistono nelle seguenti fasi:

- al Richiedente viene chiesto di presentare un valido documento di identità con fotografia rilasciato da un'autorità governativa. L'operatore esamina il documento in tempo reale tramite flusso video o immagini ad alta risoluzione, verificando:
  - Autenticità e integrità del documento (elementi di sicurezza, layout, ologrammi, ecc.)
  - Coerenza dei dati del documento (nome, data di nascita, data di scadenza);
  - Leggibilità e chiarezza della zona MRZ, ove applicabile.
- esaminare i risultati del sistema automatizzato di liveness detection;
- esaminare i risultati del confronto facciale automatizzato (face match) mediante confronto visivo tra:
  - Il volto in tempo reale del Richiedente (acquisito tramite video o immagine);
  - La fotografia presente sul documento di identità.

Qualora l'operatore riscontri incertezze riguardo ai controlli eseguiti sul processo, sospenderà o rifiuterà l'identificazione, scalerà la pratica a un supervisore per ulteriori chiarimenti.
L'operatore adotta decisioni documentate in merito all'esito della verifica dell'identità. La sessione, comprensiva delle evidenze (video, screenshot, metadati), viene registrata e conservata in modo sicuro in conformità con i requisiti normativi applicabili (ad es. GDPR, eIDAS).

3.5 Evidenze di identificazione

Al termine del processo di identificazione remota, il sistema genera e conserva le evidenze associate alla sessione di identity proofing, inclusi gli esiti dei controlli documentali, biometrici e antifrode, i riferimenti temporali e gli elementi necessari a garantire tracciabilità, integrità e auditabilità del processo.

I documenti e le evidenze sono archiviati digitalmente in un sistema di conservazione sicuro, garantendo autenticità, integrità, disponibilità e recuperabilità dei documenti archiviati per il periodo previsto dalla normativa locale.

Viene mantenuto un **audit trail** che documenta le fasi dell'intero processo di identificazione, registrando in ordine cronologico ogni stato ed evento rilevante, al fine di garantire la piena tracciabilità e responsabilità delle operazioni di verifica dell'identità.
Vengono inclusi metadati per tutte le fasi chiave del processo, quali l'acquisizione del documento, l'estrazione dei dati, l'analisi biometrica, il rilevamento della presenza fisica, i punteggi di affidabilità generati dal sistema, l'intervento manuale (ove applicabile) e l'esito finale della verifica.
Ogni evento dell'audit trail è conservato in modo sicuro e protetto da manomissioni, attraverso l'apposizione di un sigillo elettronico qualificato (eSeal), ed è disponibile per

revisioni interne o attività di audit esterno, in linea con i requisiti legali e normativi applicabili. L'audit trail, dunque, consente la ricostruzione dell'intera sessione di identificazione, garantendo trasparenza, affidabilità e conformità.

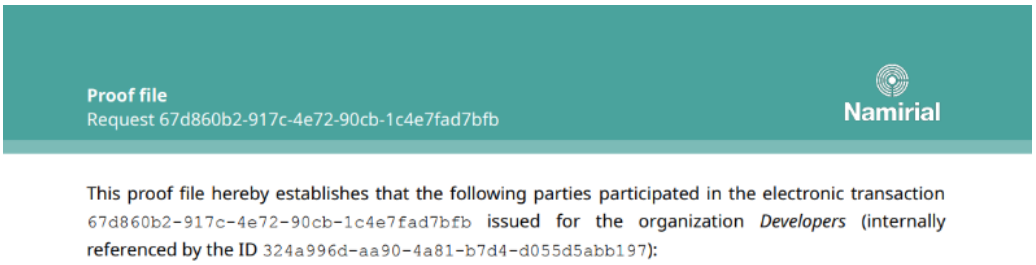

Figura 5: parte superiore dell'Audit Trail (file di prova)

A titolo esemplificativo, l'audit trail include i seguenti elementi:

- Data e ora di creazione della richiesta;
- Data e ora di accesso del Richiedente al processo NOB,
- Browser e IP del Richiedente,
- Data e ora di accettazione dei termini e condizioni;
- Data e ora di ciascuno stato di invio del documento;
- Dettagli del documento di identità presentato dal Richiedente;
- Dettagli della validazione.

I dati e le evidenze sono archiviati per un periodo definito in conformità con la normativa applicabile, al fine di garantirne la recuperabilità nel medesimo periodo da parte di personale autorizzato.

4 SOLUZIONI NAMIRIAL ONBOARDING

La suite NOB è strutturata in modo flessibile e modulare; i moduli tecnologici consentono, singolarmente o in combinazione, di creare un processo di onboarding remoto sicuro, conforme e scalabile.

4.1 Identificazione con *eID LoA sub e ID Self Fast*

Questo flusso di identificazione combina l'autenticazione tramite eID di livello significativo con la verifica documentale e i controlli biometrici. L'intervento dell'operatore viene attivato solo come fallback in caso di mancata corrispondenza dei dati.

Il processo viene avviato dal Richiedente tramite autenticazione con credenziali di identificazione elettronica preesistente che soddisfino un livello di garanzia significativo,

come SPID Livello 2 per i richiedenti italiani. Tale modalità viene considerata un fattore di ingresso alla procedura di identificazione.
A seguito dell'autenticazione, viene chiesto di effettuare un breve video in tempo reale del documento d'identità, che deve essere fisicamente in possesso del Richiedente stesso. Il documento deve essere correttamente inquadrato per consentire al sistema un'acquisizione e una verifica accurate sia del fronte sia del retro.

Il documento acquisito è sottoposto alla tecnologia OCR che estrae automaticamente i dati personali riportati nel documento stesso; vengono inoltre eseguiti controlli specifici sulla MRZ. Il sistema effettua una cross-validazione con i dati eID.

Ulteriori controlli effettuati dal sistema sono:

- Verifica della qualità dell'immagine;
- Validazione degli elementi di sicurezza del documento;
- Confronto del template con un database di documenti;
- Utilizzo di algoritmi di rilevamento delle frodi.

Completata questa prima fase, si esegue una **passive liveness detection** per verificare che la persona che presenta il documento di identità sia fisicamente presente e non stia tentando di ingannare il sistema tramite fotografie, video o deepfake. Il meccanismo funziona analizzando specifici segnali biometrici acquisiti durante una breve sessione video da cui si estrae un selfie, senza richiedere interazione attiva dell'utente. Questa fase è fondamentale per confermare che l'individuo sia il legittimo titolare del documento.
Viene effettuato un confronto biometrico tra il selfie acquisito e l'immagine del volto precedentemente estratta dal documento d'identità. Questo processo di face matching viene condotto utilizzando algoritmi biometrici (confronto 1:1) che calcolano un punteggio di affidabilità rappresentativo del grado di similarità tra le due immagini.
Se il punteggio raggiunge o supera la soglia definita, il confronto è considerato riuscito; in caso contrario, un operatore viene rapidamente coinvolto nell'esecuzione della verifica manuale. I risultati vengono forniti in meno di 5 minuti.

Scenario	Condizione generale	Azione
Approvato (Automatico)	Tutti i controlli superati senza discrepanze nei dati	Identità dell'utente verificata, processo completato senza intervento dell'operatore
Approvato (Manuale)	Discrepanza nei dati risolta con approvazione dell'operatore	Identità dell'utente verificata dopo revisione dell'operatore

Rifiutato	Controlli non superati O discrepanza irrisolta O rifiuto dell'operatore	Identità dell'utente non verificata, processo terminato

Figura 6: Scenario del caso d'uso – eID LoA sub e ID Self Fast

Le evidenze gestite in questo flusso sono:

- Asserzione eID (contiene i dati personali del titolare dell'eID);
- Immagini (e video) del documento di identità;
- Dati estratti dal documento di identità;
- Dati biometrici (immagine e video del volto dell'utente);
- Contatti dell'utente;
- Log procedurali con i controlli dell'operatore (se presenti) e azioni IDSelf.

4.2 Identificazione con *eID LoA high*

Questo flusso di identificazione prevede un onboarding completamente automatizzato e si avvale dell'autenticazione tramite strumenti di identità elettronica nazionale di livello elevato (eID Livello 3 eIDAS). Non è richiesta né l'acquisizione del documento di dientità né la verifica biometrica, tantomeno l'intervento di un operatore.

Il processo viene avviato dal Richiedente tramite autenticazione con credenziali di identificazione elettronica preesistente che soddisfino un livello di garanzia elevato, come CIE Livello 3 per i richiedenti italiani.

Il processo è altamente efficiente, in quanto supportato dalla **federazione dell'identità digitale** consentendo autenticazione tra i sistemi senza soluzione di continuità. L'autenticazione di livello elevato consente il trasferimento sicuro dei dati personali del Richiedente al sistema, tramite interazione con fonti autorevoli, come i database CIE Livello 3. Questa connessione diretta riduce significativamente l'inserimento manuale, minimizza il rischio di errori e garantisce l'accuratezza dei dati di identità fin dall'inizio.

Grazie a questa tipologia di autenticazione, il processo di verifica dell'identità è considerato completato con successo e conforme ai requisiti di garanzia applicabili.

Scenario	Condizione Generale	Azione
Approvato	Autenticazione eID Livello 3 completata con successo	Identità verificata, processo completato automaticamente
Rifiutato	Autenticazione eID fallita o livello eID non valido	Identità non verificata, processo terminato

Figura 7: Scenario del caso d'uso – eID LoA high

Le evidenze gestite in questo flusso sono:

- Asserzione eID (contiene i dati personali del titolare dell'eID);
- Contatti dell'utente;
- Log procedurali.

4.3 Identificazione con *ID Self Trust*

Questo flusso di identificazione utilizza l'acquisizione del documento di identità, la verifica biometrica con liveness detection e la revisione obbligatoria da parte dell'operatore in tutti i casi.

Il processo ha inizio con l'acquisizione del documento di identità del Richiedente. Questa fase iniziale garantisce che il documento sia in possesso del richiedente, sia valido e autentico.
Il documento deve essere chiaramente inquadrato in tempo reale, per consentire un'acquisizione e una verifica accurate da parte del sistema (fronte e retro). Il documento acquisito è sottoposto alla tecnologia OCR che estrae automaticamente le informazioni personali essenziali; vengono eseguiti controlli specifici sulla MRZ.

Successivamente, il sistema esegue la **passive liveness detection** per verificare che la persona che presenta il documento di identità sia fisicamente presente e non stia tentando di ingannare il sistema. Il sistema analizza i segnali biometrici acquisiti durante una breve sessione video, senza richiesta di interazione attiva dell'utente.

A seguire, è obbligatorio l'intervento di un operatore di back-office esperto, per revisionare e verificare il corretto campionamento del documento.

Di seguito una panoramica dei controlli eseguiti dall'operatore:

- validazione dei dati estratti dal documento di identità, garantendo coerenza e accuratezza.
- validazione della MRZ, per verificarne l'integrità e confermare che le informazioni corrispondano ai dati stampati sul documento;
- verifica e conferma del confronto facciale;
- chiusura della richiesta con produzione del report finale

Gli operatori di back-office effttuano le operazioni di verifica manuale 24/7, i risultati sono disponibili in meno di 5 minuti.

Scenario	Condizione Generale	Azione
Approvato	Tutti i controlli superati e approvazione aggiuntiva dell'operatore	Identità dell'utente verificata, processo completato
Rifiutato	Controlli non superati o rifiuto da parte dell'operatore	Identità dell'utente non verificata, processo terminato

Figura 8: Scenario del caso d'uso – ID Self Trust

Le evidenze gestite in questo flusso sono:

- Immagini (e video) del documento di identità;
- Dati estratti dal documento di identità;
- Dati biometrici (immagine e video del volto dell'utente);
- Contatti dell'utente;
- Log procedurali con controlli dell'operatore e azioni ID Self.

4.3.1 Identificazione con *ID Self Trust (con challenge)*

Questo processo di identificazione comprende tutti i controlli avanzati descritti nel paragrafo precedente, con l'aggiunta di **challenge.** Le challenge attive consistono nella richiesta di specifiche azioni o movimenti casuali del volto, la cui corretta esecuzione viene verificata mediante analisi biometrica e correlazione temporale, al fine di prevenire attacchi di replay, spoofing, deepfake e video injection.

Scenario	Condizione generale	Azione
Approvato	Tutti i controlli superati, challenge attiva completata con successo e approvazione dell'operatore	Identità dell'utente verificata con livello di certificazione IAD high
Rifiutato (Automatico)	Challenge attiva non superata o inattività rilevata, o mancata conformità dei movimenti	Processo terminato, utente notificato
Rifiutato (Operatore)	L'operatore individua indicatori di frode o rifiuto dell'operatore a seguito di revisione	Identità dell'utente non verificata, processo terminato

Figura 9: Scenario del caso d'uso – ID Self Trust con challenge

4.4 Identificazione con *ID Doc, tecnologia NFC e ID Face*

Questo processo di identificazione prevede un flusso avanzato di onboarding che combina acquisizione del documento di identità, lettura del chip NFC nei documenti elettronici e verifica biometrica facciale. L'intervento dell'operatore è attivato unicamente come fallback nei casi di mancata corrispondenza o insufficiente affidabilità del risultato del face matching.

Il processo è basato su un documento di identità digitale ed è strutturato in aderenza allo standard eMRTD (ICAO Doc 9303). Il processo ha inizio con l'acquisizione della MRZ del documento di identità, dalla quale viene derivata la access key (BAC or PACE key). Questa chiave consente di stabilire una comunicazione sicura con il chip integrato nel documento, conforme agli standard ICAO, dal quale vengono acquisiti gli attributi identificativi del titolare, inclusi l'immagine facciale e gli altri dati anagrafici contenuti nel documento.

L'autenticità e l'integrità dei dati estratti dal chip sono verificate tramite autenticazione passiva, garantendo che il documento sia stato emesso da un'autorità riconosciuta e non sia stato alterato.

Successivamente, al Richiedente viene chiesto di eseguire una sequenza di *liveness detection* passiva tramite la fotocamera del proprio dispositivo. Dal flusso video acquisito viene automaticamente estratto un frame rappresentativo, che viene confrontato con l'immagine facciale ottenuta dal chip dell'eMRTD mediante algoritmi di face matching.
Il riscontro positivo tra le due immagini consente di stabilire un *binding* sicuro e affidabile tra la presenza fisica del Richiedente e gli attributi di identità estratti dal documento di identità elettronico.

Se il punteggio raggiunge o supera la soglia definita, il confronto è considerato riuscito; in caso contrario, un operatore viene rapidamente coinvolto nell'esecuzione della verifica manuale. I risultati vengono normalmente forniti in meno di 5 minuti.

Scenario	Condizione generale	Azione
Approvato (Automatico)	Tutti i controlli superati e confronto facciale riuscito	Identità dell'utente verificata, processo completato senza intervento dell'operatore
Approvato (Manuale)	Discrepanza facciale risolta con approvazione dell'operatore	Identità dell'utente verificata dopo revisione dell'operatore

Rifiutato	Controlli non superati o autenticazione NFC fallita, o discrepanza irrisolta, o rifiuto dell'operatore	Identità dell'utente non verificata, processo terminato

Figura 10: Scenario del caso d'uso – ID Doc, NFC e ID Face

Le evidenze gestite in questo flusso sono:

- Immagini (e video) del documento di identità
- Dati estratti dal documento di identità
- Dati biometrici (immagine e video del volto dell'utente)
- Dati estratti dalla lettura NFC del documento, inclusa l'immagine del volto del titolare;
- Contatti dell'utente;
- Log procedurali con controlli dell'operatore e azioni ID DOC/ID Face/ID NFC

4.5 Identificazione con *Namirial Wallet*

L'EUDI Wallet può essere inteso come un contenitore digitale sicuro che consente agli utenti di archiviare e gestire in modo protetto dati personali o organizzativi direttamente sui propri dispositivi (mobile o web-based). Tale soluzione innovativa rientra negli sforzi in corso della Commissione europea volti a rafforzare la sicurezza, la tutela della privacy e l'interoperabilità delle identità digitali tra gli Stati membri dell'Unione europea.

Questo flusso di identificazione prevede un onboarding completamente automatizzato, non è richiesta né l'acquisizione del documento né la verifica biometrica tantomeno l'intervento di un operatore di back-office. Il richiedente apre l'app Digital Wallet, scansiona il codice QR, o segue il deep link, e autorizza la presentazione della credenziale PID.

Namirial Wallet include un **dato di identificazione personale (PID),** emesso sulla base di un processo di enrollment e verifica dell'identità eseguito da Namirial ai sensi dei paragrafi precedenti e coerente con la bozza FprCEN/TS 18098 di luglio 2025, collegato a una coppia di chiavi conservata in modo sicuro su un HSM remoto certificato. Il Dispositivo Crittografico Sicuro del Wallet (Wallet Secure Cryptographic Device – WSCD) è conforme al livello di assurance AVA_VAN.5 e si basa su un modulo HSM certificato Common Criteria con livello EAL4+. Esso garantisce il controllo esclusivo da parte dell'utente sulle coppie di chiavi associate alla Wallet Unit.

Namirial Wallet funge da equivalente di uno strumento eID di livello LoA High, utilizzato per l'autenticazione forte e continuativa dell'identità precedentemente verificata da Namirial.

Il Wallet è utilizzato esclusivamente per l'erogazione di servizi di identità digitale e fiduciari forniti da Namirial o da partner contrattuali operanti nell'ecosistema di servizi Namirial. Di conseguenza, il Namirial Wallet non costituisce uno schema di identificazione elettronica (eID) notificato ai sensi dell'articolo 9 del Regolamento eIDAS, bensì una credenziale e uno schema proprietario di livello di fiducia elevato.

Il sistema riceve e valida il PID dal Wallet dell'utente; il processo si conclude immediatamente dopo l'autenticazione Wallet e la validazione del PID avvenute con successo.

Scenario	Condizione generale	Azione
Approvato	Autenticazione Wallet riuscita, validazione PID riuscita e tutte le prove crittografiche valide	Identità dell'utente verificata con livello di garanzia elevato, processo completato automaticamente
Rifiutato	Autenticazione Wallet fallita o credenziale PID non valida/scaduta, o verifica della firma fallita, o credenziale revocata	Identità dell'utente non verificata, processo terminato con codice di errore

Figura 11: Scenario del caso d'uso – Namirial Wallet

Dopo l'enrollment, il Wallet e il Namirial PID vengono utilizzati per autenticare il richiedente per molteplici finalità, incluso il rilascio di certificati digitali qualificati.

Le evidenze di enrollment gestite sono:

- Asserzione PID (Presentazione Verificabile): contiene dati personali con livello di garanzia elevato (cognome, nome, data di nascita, luogo di nascita, nazionalità, identificativo univoco);
- Prove Crittografiche: Firme JWT, catene di certificati, valori nonce;
- Informazioni di Contatto dell'Utente: indirizzo e-mail e numero di telefono verificati;
- Log Procedurali:
    - Eventi del flusso di autenticazione OID4VP
    - Timestamp per tutte le fasi critiche
    - Informazioni sul provider del Wallet
    - Informazioni sull'emittente del PID
    - Registrazioni del consenso dell'utente
    - Parametri di sicurezza della sessione

5 CONTROLLI E MISURE DI SICUREZZA

5.1 Controlli di sicurezza fisica

Namirial ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) in linea con lo standard internazionale per la sicurezza delle informazioni ISO/IEC 27001.
Opera, inoltre, per tutti i siti di erogazione, in conformità alle proprie policy di sicurezza di gruppo SCS-P05 Group Information Security Operational Policy, progettate per rilevare, scoraggiare e prevenire accessi non autorizzati alle operazioni dell'Organizzazione.

Nell'ambito dell'erogazione del servizio oggetto del presente documento, le misure di sicurezza delle informazioni sono coerenti con le certificazioni conseguite.

5.1.1 Accesso fisico

Tali misure si applicano alle strutture da cui viene erogato il servizio, nei rispettivi ambienti di produzione e di contingenza, che sono periodicamente sottoposte ad audit nel rispetto della normativa applicabile e delle policy interne di Namirial.

5.1.1.1 Ubicazione del sito

I data center di produzione sono gestiti da:

- Amazon AWS, in Irlanda, Dublino: certificati ISO 27001, SOC 1/2/3 e PCI DSS);
- FreePro, in Francia, Marsiglia e Lione: certificati ISO 27001 / PCI-DSS / HDS e con processo avviato di qualificazione SecNumCloud.

Tali certificazioni garantiscono che entrambi i siti aderiscano a rigorosi controlli di sicurezza e processi di gestione del rischio.

5.1.1.2 Controlli di accesso fisico

Le strutture attraverso cui viene erogato il servizio sono ridondanti e protette da misure che impediscono l'accesso non autorizzato ai dati e la loro divulgazione.
La protezione fisica viene conseguita mediante l'implementazione di perimetri di sicurezza chiaramente definiti attorno al servizio, quali sistemi antintrusione passivi con barriera attorno all'edificio e porte di sicurezza rinforzate.
Sono implementati tre livelli di controllo degli accessi, da raggiungere progressivamente, incluso il rilevamento biometrico (lettore di impronte digitali).
L'accesso è strettamente limitato al personale espressamente autorizzato, che deve essere identificato all'ingresso e registrato. Il sistema registra automaticamente gli ingressi e le uscite.
Si aggiungono sistemi antintrusione attivi, quali sistema di allarme e videosorveglianza costante degli spazi interni ed esterni.

Le strutture dispongono di sistemi di manutenzione preventiva e correttiva con assistenza 24 ore su 24, 365 giorni l'anno, e interventi entro 24 ore dalla segnalazione.

5.1.2 Impianto elettrico e climatizzazione

Le sale che ospitano le apparecchiature informatiche sono dotate di un'infrastruttura elettrica altamente sicura e ridondante, inclusi sistemi di stabilizzazione dell'alimentazione e doppia alimentazione con generatore. L'intera configurazione garantisce la disponibilità continua dell'energia, con ridondanza N+2. La struttura dispone inoltre di sistemi avanzati di controllo della temperatura.

5.1.3 Prevenzione e protezione antincendio

Le principali infrastrutture e asset dei data center (DC) sono dotati di sistemi automatici di rilevazione e spegnimento degli incendi.

5.1.4 Protezione da allagamenti

Le strutture sono ubicate in una zona a basso rischio di allagamento. Le sale che ospitano le apparecchiature informatiche sono dotate di un sistema di rilevamento dell'umidità e di sensori che rilevano la presenza di liquidi e attivano un allarme in caso di allagamento.

5.1.5 Media handling

Le risorse sono protette da danni accidentali e da accessi fisici non autorizzati. Solo il personale autorizzato ha accesso alla gestione e ai supporti di archiviazione. Le informazioni altamente riservate vengono conservate in modo sicuro in una cassaforte esterna.
La rimozione dei supporti, sia cartacei che magnetici, viene effettuata mediante meccanismi che garantiscono l'irrecuperabilità delle informazioni.

5.2 Controlli procedurali

Tutte le procedure relative alla sicurezza nell'erogazione del servizio, incluse l'identificazione e la verifica di attributi specifici per il rilascio, la gestione e l'utilizzo di certificati qualificati di firma elettronica, sono svolte da personale fidato di Namirial. Viene sempre garantito un numero sufficiente di dipendenti qualificati per assicurare il rispetto della normativa applicabile e delle policy e procedure interne.

5.2.1 Trusted roles

Sono nomitati i trusted roles previsti dallo standard ETSI EN 319-401, possiedono la necessaria esperienza, professionalità e competenza tecnica. Ricevono inoltre il livello di formazione necessario sulle procedure e sugli strumenti utilizzabili nelle varie fasi operative.

Tutto il personale nominato secondo trusted roles deve essere libero da conflitti di interesse che possano essere pregiudizievoli a livello di imparzialità nelle operazioni svolte da ciascuno nell'esercizio delle proprie funzioni.
I trusted roles sono nominati dal management. Un elenco del personale nominato in tali ruoli viene mantenuto e rivisto dall'Organizzazione, in un apposito documento di Struttura organizzativa, che viene mantenuto e rivisto da Namirial, nonché inviato ad ogni aggiornamento all'Organismo di Vigilanza.

5.3 Controlli sul personale

Tutto il personale coinvolto nell'erogazione del servizio possiede adeguata esperienza nella definizione, sviluppo e gestione del servizio e riceve, con cadenza regolare, il necessario livello di formazione su procedure e strumenti che possono essere utilizzati in varie fasi operative.

Il personale Namirial incaricato a queste attività deve:

- possedere la competenza, l'affidabilità, l'esperienza e le qualifiche necessarie e aver ricevuto formazione relativa alle norme di sicurezza e di protezione dei dati personali adeguata ai servizi offerti e alla loro funzione lavorativa;
- essere in grado di soddisfare il requisito di "conoscenza, esperienza e qualifiche" attraverso formazione o esperienza effettiva, o una combinazione di entrambe;
- essere aggiornato circa le nuove minacce e sulle più recenti pratiche di sicurezza applicabili.

Namirial assume personale con i più alti livelli di integrità e competenza. Non esiste alcun requisito di cittadinanza per il personale coinvolto nell'erogazione del servizio.

5.3.1 Check delle esperienze pregresse

Namirial verifica l'identità ed esegue un controllo delle esperienze pregresse di ogni dipendente al fine di affidare uno dei trusted roles previsti ed indicati in precedenza

5.3.2 Check delle esperienze in itinere

La funzione aziendale delle Risorse umane, con il supporto dei Responsabili dei servizi, implementa un processo di monitoraggio continuo delle competenze e delle performance del personale. Il processo prevede l'assegnazione di specifici obiettivi definiti in base al ruolo ricoperto, nonché il monitoraggio periodico dello stato di avanzamento e della percentuale di raggiungimento degli stessi.
A supporto di tale monitoraggio, i Responsabili di servizio organizzano incontri periodici one-to-one con le risorse del proprio team, finalizzati a verificare l'adeguatezza delle competenze rispetto al ruolo assegnato e intervenire tempestivamente in caso di scostamenti o necessità di rafforzamento.

L’analisi continua delle competenze consente, inoltre, di valutare la corretta allocazione delle risorse e di definire programmi di formazione annuale, volti a colmare eventuali gap emersi e a rafforzare la consapevolezza del personale sulle politiche e procedure rilevanti.
Attraverso tali presidi, Namirial assicura che le risorse coinvolte nell’erogazione dei servizi siano costantemente monitorate nel tempo e mantengano un livello di competenza adeguato

5.3.3 Requisiti di formazione

Il personale Namirial riceve una formazione di base in materia di sicurezza delle informazioni e consapevolezza sulla protezione dei dati fin dalle prime fasi del processo di onboarding aziendale. Tale formazione viene successivamente riproposta con cadenza regolare (almeno annuale) attraverso la somministrazione di video-lezioni, corredate da appositi test di verifica dell’apprendimento.

I corsi obbligatori comprendono, in particolare, i seguenti ambiti tematici:

- GDPR e Data Protection (selezionati dal DPO)
- Security Awareness (selezionati dal CISO)

Le funzioni responsabili della verifica della formazione (Risorse umane, DPO, CISO e Responsabili delle Business unit) dispongono di strumenti di analisi e monitoraggio dello stato di completamento dei percorsi formativi, sopra citati, da parte del personale. Oltre a ciò, una formazione on-the-job dedicata viene fornita a tutto il personale Namirial coinvolto in compiti specifici, come descritto nel presente documento.

5.3.4 Frequenza di aggiornamento della formazione e requisiti

Il personale è tenuto a mantenere elevati livelli di competenza attraverso sessioni di formazione pertinenti al settore, al fine di continuare ad agire in conformità con i requisiti del proprio ruolo.

All'inizio di ogni anno vengono analizzati i fabbisogni formativi per definire i corsi da erogare. L'analisi si basa sui seguenti passaggi:

- Incontro con la direzione aziendale per raccogliere dati sui fabbisogni formativi necessari al raggiungimento degli obiettivi.
- Feedback dei responsabili delle business unit per identificare i fabbisogni formativi specifici di ciascun dipartimento.
- Presentazione dei dati raccolti alla direzione aziendale per la finalizzazione e l'approvazione del Piano Formativo.

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

5.3.5 Frequenza della job rotation

In caso di rotazione dei ruoli, Namirial esegue un controllo di sicurezza, inclusa una verifica delle credenziali a livello di reti, sistemi, applicazioni o altre risorse utilizzate, nonché delle autorizzazioni di accesso alle strutture e alle aree.

5.3.6 Requisiti per il personale non dipendente

Il personale non dipendente è soggetto ai requisiti e agli obblighi specifici del ruolo, nonché alle relative sanzioni.

5.3.7 Documentazione fornita al personale

Al personale inserito vengono fornite le informazioni necessarie per svolgere le proprie mansioni, inclusa una copia del presente documento e la documentazione operativa necessaria per mantenere l'integrità delle operazioni.

5.3.8 Sanzioni per azioni non autorizzate

Il personale Namirial che non rispetta le policy e le disposizioni interne dell'organizzazione, per negligenza o in modo doloso, è soggetto a sanzioni amministrative o disciplinari, inclusa la risoluzione del rapporto di lavoro o di collaborazione e, nei casi più gravi, sanzioni penali.

5.4 Procedure per la registrazione di eventi e file di log

Gli eventi generati dal sistema durante le fasi del processo del servizio di certificazione e validazione temporale producono dei log, che consentono di tracciare le diverse operazioni che si verificano durante i processi automatici e di interazione con l'utente, facilitando la diagnosi di eventuali anomalie e/o incidenti

5.4.1 Tipi di eventi registrati

Namirial produce e conserva registrazioni almeno dei seguenti eventi relativi alla sicurezza del sistema:

- Attivazione e spegnimento del sistema;
- Manutenzione e modifiche delle impostazioni di sistema;
- Tentativi di creare, eliminare, impostare password o modificare privilegi;
- Modifiche relative alla gestione degli account con privilegi;
- Tentativi di accesso non autorizzato ai sistemi attraverso la rete;
- Tentativi di accesso non autorizzato al file system;
- Accesso ai log;
- Registrazioni della distruzione dei supporti, compresi quelli contenenti le chiavi crittografiche e i dati di attivazione;

- Eventi relativi al ciclo di vita del modulo crittografico;
- La cerimonia di generazione delle chiavi e i database di gestione delle stesse;
- Registri di accesso fisico;
- Rapporti completi dei tentativi di intrusione fisica nelle infrastrutture che supportano il servizio;
- Rapporti di compromissioni e discrepanze;
- Eventi relativi alla sincronizzazione e ricalibrazione dell'orologio

Con riferimento al processo di Onboarding gli eventi raccolti e registrarti sono:

- Dati personali del richiedente
- Fotografia del fronte del documento di identità
- Fotografia del retro del documento di identità
- Fotografia del volto estratta dal documento di identità
- Fotografia del volto estratta dal video biometrico
- Video biometrico originale
- Video originale del documento di identità

Informazioni di audit e logging:

- Audit trail
- Log delle attività dell'operatore, che deve includere:
    - Nome completo dell'operatore
    - ID utente dell'operatore
    - Evidenza delle azioni eseguite con riferimenti temporali
    - Chi ha eseguito l'azione, quale azione, quando e per quanto tempo
- Log contenenti le versioni di tutti i moduli coinvolti

I log includono i seguenti elementi:

- Data e ora dell'evento;
- Numero di serie o sequenza dell'evento, nei registri automatici;
- utente che esegue l'evento;
- Tipo di evento.

5.4.2 Frequenza di salvataggio ed elaborazione dei log

L'elaborazione dei log consiste nella loro revisione periodica, finalizzata a verificarne l'integrità e ad analizzare le registrazioni presenti, con particolare attenzione ad alert o anomalie. Eventuali approfondimenti e le azioni conseguenti sono formalmente documentati.

Namirial mantiene un sistema che permette di garantire:

- spazio sufficiente per la memorizzazione dei log;
- che i file di log non siano sovrascritti;

- che le informazioni salvate includano almeno: tipo di evento, data e ora, utente che esegue l'evento e risultato dell'operazione.

I file di log sono archiviati in file strutturati che possono essere incorporati in un database per esplorazioni successive.

La frequenza di salvataggio dell'audit log è giornaliera. L'ora utilizzata per registrare gli eventi deve essere sincronizzata con UTC almeno una volta al giorno.

5.4.3 Conservazione dei registri

Namirial produce e mantiene registri accessibili che includono tutte le attività e tutte le informazioni rilevanti relative ai dati emessi e ricevuti da Namirial. La procedura predisposta dal QTSP prevede che gli eventi rilevati e disponibili nel database vengano estratti e inseriti in file di testo gestiti in modo da garantirne l'integrità e la disponibilità.
Le evidenze generate durante il processo di verifica dell'identità sono conservate in modo a prova di manomissione, garantendo la riservatezza delle informazioni. Le evidenze sono archiviate nel sistema di Archiviazione a Lungo Termine di Namirial (LTA).
Qualora il processo di onboarding venga utilizzato per l'emissione di certificati qualificati di firma elettronica, i dati e le evidenze vengono archiviati per 20 (venti) anni, in conformità con la normativa italiana.
I registri relativi all'operatività dei servizi sono messi a disposizione dell'autorità giudiziaria in caso di procedimenti legali e, internamente, ai fini di audit e verifiche periodiche del sistema.
Tali registri rimangono accessibili anche nel caso in cui Namirial abbia cessato le proprie attività.

5.4.4 Protezione dei file

I file sono protetti in modo tale che solo il personale debitamente autorizzato possa accedervi. Sono salvaguardati da visualizzazioni, modifiche, cancellazioni o qualsiasi altra forma di manomissione, in quanto conservati all'interno di un sistema fidato. Namirial garantisce un'adeguata protezione dei file assegnando personale qualificato al loro trattamento e archiviandoli in strutture esterne sicure.

5.4.5 Procedure di backup

Namirial dispone di un'adeguata procedura di backup che garantisce che, in caso di perdita o distruzione dei file rilevanti, le corrispondenti copie di backup dei log siano disponibili entro un breve lasso di tempo.

5.4.6 Sistema di archiviazione dei log

Le informazioni relative ai log vengono raccolte internamente e automaticamente dal sistema, dalle comunicazioni di rete e dal software di servizio, oltre ad eventuali dati generati manualmente, che verranno archiviati dal personale debitamente autorizzato.

5.4.7 Notifica dell'evento di audit al causatore dell'evento

Quando il sistema di archiviazione dei log registra un evento, non è necessario inviare una notifica alla persona, organizzazione, dispositivo o applicazione che ha causato l'evento.

5.4.8 Analisi delle vulnerabilità

Namirial esegue periodicamente attività di vulnerability assessment e penetration test sui propri sistemi, rispettando le tempistiche indicate dagli standard di riferimento.
Sulla base dei risultati ottenuti, vengono implementate tutte le contromisure necessarie per garantire la sicurezza delle applicazioni e dei sistemi.

5.5 Archiviazione delle informazioni

Per ciascun evento rilevante vengono redatti e archiviati appositi registri.

5.5.1 Tipi di registri archiviati

La CA conserva tutte le informazioni relative a:

- tutti i dati relativi al ciclo di vita del processo di onboarding;
- le richieste di identificazione;
- documenti di identità presentati al momento della richiesta di identificazione;
- dati personali del Richiedente;
- audit trail;

5.5.2 Periodo di archiviazione

Tali registrazioni sono conservate per un periodo di 20 anni.

5.5.3 Protezione degli archivi

Namirial protegge gli archivi attraverso controlli fisici e logici di accesso, affinché solo le persone debitamente autorizzate possano accedervi. L’archivio è protetto dalla visualizzazione, la modifica, la cancellazione o qualsiasi altra manipolazione grazie all’implementazione di un sistema affidabile.

5.5.4 Backup degli archivi

Tutte le informazioni soggette a conservazione sono sottoposte a procedure di backup incrementate verso il sito di DR, al fine di garantirne disponibilità, integrità e recuperabilità in caso di incidente o indisponibilità dei sistemi primari.

5.5.5 Data e ora

I log sono datati con una fonte affidabile tramite NTP. Non è necessario che queste informazioni siano firmate digitalmente.

5.5.6 Sistema di archiviazione e conservazione delle registrazioni

Il sistema di archiviazione e conservazione delle registrazioni è gestito internamente da Namirial mediante un sistema di conservazione a norma, conforme ai requisiti normativi e di sicurezza applicabili.

5.5.7 Procedure per ottenere e verificare le informazioni di archiviazione

Le informazioni archiviate sono rese disponibili mediante procedure specifiche per la verifica e la messa a disposizione di tali informazioni

5.6 Procedure di gestione degli incidenti

Namirial ha sviluppato politiche di sicurezza e continuità aziendale che consentono la gestione e il recupero dei sistemi in caso di incidenti e compromissione delle sue operazioni. La procedura apposita per la gestione e la risposta agli incidenti, applicata anche attraverso un sistema di allerta e la generazione di rapporti periodici, è descritta in dettaglio nell'idonea documentazione interna a Namirial.

5.6.1 Corruzione di risorse, applicazioni o dati

Quando si verifica un evento di corruzione delle risorse, applicazioni o dati, vengono seguite le procedure di gestione appropriate in conformità con le politiche di sicurezza e gestione degli incidenti di Namirial, che includono escalation, indagine e risposta all'incidente. Se necessario, vengono attivate le procedure di compromissione delle chiavi o di recupero dai disastri di Namirial.

5.6.2 Continuità aziendale dopo un disastro

Namirial ripristinerà i servizi critici in conformità con il piano di continuità aziendale relativo al servizio, ripristinando il normale funzionamento dei servizi precedenti entro un massimo di 24 ore dal disastro.

5.7 Piano di Cessazione del Servizio

Namirial ha definito un piano di cessazione aggiornato per il servizio oggetto del presente documento, che verrà implementato qualora si presenti la necessità.

Il documento contiene le seguenti disposizioni:

- disposizione dei fondi necessari, inclusa l'assicurazione di responsabilità civile, per eseguire l'attività di cessazione;
- comunicazione all'Autorità di Vigilanza, a tutti i sottoscrittori del servizio, alle Terze Parti e in generale ogni terza parte con cui si hanno accordi o altro tipo di rapporto con un anticipo minimo di 3 (tre) mesi;
- esecuzione delle attività necessarie per trasferire gli obblighi di manutenzione delle informazioni dei log e delle evidenze per i rispettivi periodi di tempo.

6 CONTROLLI DI SICUREZZA TENICA

6.1 Utilizzo della crittografia per la sottoscrizione delle evidenze del processo di identificazione (*audit trail*)

Le evidenze del processo di identificazione (audit trail) sono protette mediante meccanismi crittografici che ne garantiscono autenticità, integrità e immodificabilità nel tempo.

A tal fine, ogni audit trail è sottoscritto con sigillo elettronico qualificato del QTSPNamirial, in conformità al Regolamento eIDAS. Il sigillo elettronico qualificato è basato su un certificato qualificato e su una coppia di chiavi crittografiche (chiave privata e chiave pubblica).

L'uso della crittografia costituisce quindi un elemento tecnico fondamentale per garantire il valore probatorio degli audit trail e la loro affidabilità nel tempo.

6.2 Controlli di sicurezza informatica

La strumentazione utilizzata viene configurata con i profili di sicurezza appropriati, dal personale dei sistemi di Namirial, nei seguenti aspetti:

- configurazione di sicurezza del sistema operativo;
- impostazioni di sicurezza delle applicazioni;
- dimensionamento corretto del sistema;
- configurazione degli utenti e dei permessi;
- configurazione degli eventi di registro;
- piano di backup e recupero;
- requisiti del traffico di rete;
- controlli del ciclo di vita tecnico;
- controlli sullo Sviluppo del Sistema.

I sistemi operativi utilizzati da Namirial per la gestione dell'erogazione del servizio hanno un elevato livello di sicurezza e seguono le procedure di hardening stabilite da Namirial.
I compiti e le aree di responsabilità sono segregati al fine di minimizzare la possibilità di modifiche non autorizzate o utilizzo improprio delle risorse di Namirial.
Gli eventi di accesso ai sistemi vengono registrati; le componenti della rete locale vengono mantenute in un ambiente sicuro e le configurazioni vengono periodicamente verificate per la conformità ai requisiti specificati da Namirial.
Vengono implementati job automatizzati per verificare l'integrità del software e della relativa configurazione.
Sono implementati sistemi di monitoraggio continuo e alert per consentire a Namirial di rilevare, registrare e rispondere tempestivamente a qualsiasi tentativo non autorizzato e/o irregolare di accesso alle proprie risorse.

6.3 Controlli di network security

L'architettura di rete di Namirial è strutturata su più livelli in modo da creare ambienti di rete separati, indirizzati a host relativi a funzioni diverse e caratterizzati da diversi livelli di criticità.
La sicurezza degli accessi e del traffico di rete è garantita mediante l'applicazione di politiche di protezione implementate sui sistemi firewall dislocati su diversi livelli di rete.
Le richieste di implementazione di nuove regole sul firewall sono gestite attraverso una change request.
L'attivazione di regole che causano un alto livello di impatto, viene trattata con il Security Officer. La sicurezza della rete privata è realizzata non solo dai sistemi di protezione perimetrale descritti in precedenza, ma anche da una configurazione specifica che mantiene gli indirizzi interni come riservati. Le comunicazioni tra le stazioni di gestione e i sistemi sono protette per mezzo di strumenti che assicurano l'autenticazione tra le parti e la loro privacy.
I potenziali collegamenti remoti avvengono su un canale VPN criptato e richiedono l'autenticazione (MFA) tramite username, password e un token di autenticazione (OTP).La

comunicazione tra i moduli applicativi della piattaforma PKI di Namirial avviene attraverso canali crittografici.
La comunicazione tra gli utenti che accedono ai servizi online avviene attraverso connessioni TLS/SSL con algoritmo SHA -256.
Il sistema implementato per gestire gli accessi degli utenti fornisce sia meccanismi AAA (autenticazione, autorizzazione, accesso) e di profilazione che la crittografia del canale di comunicazione con protocollo TLS/SSL

7 AUDIT E CONFORMITÀ

Namirial è un Qualified Trust Service Provider soggetto ad attività periodica di valutazione della conformità del servizio da parte di un Organismo di Valutazione della Conformità (CAB), riconosciuto in ambito UE.

Namirial è anche soggetta ad una valutazione di conformità ("sorveglianza") da parte dell'Organismo di Vigilanza AgID

7.1 Frequenza e circostanze della valutazione di conformità

La funzione di audit di Namirial è responsabile degli audit interni sul servizio oggetto del presente documento, che si occupa di verificare che i processi siano conformi ai requisiti di legge, al Regolamento eIDAS nonché agli standard tecnici che regolano l'erogazione del servizio. L'audit interno viene effettuato almeno una volta all'anno.

L'audit di terza parte, allo stesso modo, viene eseguito da un Organismo di Valutazione della Conformità con periodicità almeno annuale.

7.2 Azioni derivanti da non conformità

In caso di non conformità, Namirial adotta le azioni correttive necessarie stabilendo un termine di risoluzione congruo rispetto alla natura e alla criticità della stessa. L'avanzamento delle attività correttive è monitorato fino alla completa chiusura.

Qualora l'Organismo di Vigilanza rilevi eventuali non conformità rispetto ai requisiti previsti dal Regolamento (UE) eIDAS, Namirial provvederà ad adottare tutte le misure correttive necessarie entro i termini indicati dall'Autorità competente.

7.3 Comunicazione dei risultati

I risultati degli audit sono condivisi con Namirial attraverso un rapporto di valutazione della conformità. Il risultato dell'audit interno, invece, viene comunicato alla Direzione e al Responsabile del Servizio, incaricato della fornitura del servizio stesso.

8 ASPETTI LEGALI E DI BUSINESS

8.1 Tariffe

Le tariffe per i servizi NOB sono disciplinate dall'accordo commerciale tra Namirial e il Partner. Nessuna tariffa è definita nel presente documento.

8.2 Responsabilità finanziaria

Namirial possiede mezzi finanziari sufficienti per mantenere le sue operazioni e adempiere ai suoi obblighi, oltre che per affrontare il rischio di responsabilità per danni, come stabilito nella ETSI EN 319 401, in relazione alla gestione del piano di cessazione dei servizi e della dismissione.

8.3 Copertura assicurativa

Namirial ha stipulato un'assicurazione di responsabilità civile professionale che comprende i servizi fiduciari qualificati descritti nel presente documento. La polizza è pubblicamente disponibile sul sito web Namirial al seguente link https://www.namirial.com/it/documentazione/

I limiti specifici di copertura assicurativa applicabili nel rapporto con i Partner sono definiti nell'Addendum.

8.4 Protezione dei dati personali

Le informazioni personali concernenti i Richiedenti del servizio e, più in generale, i clienti del servizio erogato vengono trattate, conservate e protette in conformità a quanto previsto nel Regolamento europeo 679/2016 in materia di protezione dei dati personali.
Namirial S.p.A. garantisce la tutela degli interessati, in ottemperanza al Regolamento europeo 679/2016 in materia di protezione dei dati personali. In particolare, fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.

8.4.1 Titolare del trattamento

Il titolare del trattamento dei dati personali è:

- Namirial S.p.A.
- P.IVA: IT02046570426.
- Indirizzo: Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia.

I termini e le condizioni applicabili al trattamento dei dati personali, inclusa la ripartizione delle responsabilità tra le Parti, sono disciplinati dal Contratto per il Trattamento dei Dati Personali (Data Processing Agreement – DPA), stipulato ai sensi dell'articolo 28 del GDPR e allegato all'Addendum Partner.

8.4.1.1 Dettagli di contatto dell'organizzazione responsabile della protezione dei dati

I dettagli di contatto del Responsabile della Protezione dei Dati sono:

- Website: https://www.namirial.com/it/privacy-policy/
- E-mail: dpo@namirial.com
- PEC: dpo.namirial@sicurezzapostale.it

8.4.2 Tipologia di dati trattati

Nell'ambito del servizio di identificazione e onboarding, sono trattate le seguenti categorie di dati personali:

- Dati anagrafici (nome, cognome, codice fiscale, sesso, data di nascita, luogo di nascita, nazionalità);
- Estremi e copia del documento di identità;
- Dati di indirizzo (residenza/domicilio);
- Dati di contatto (recapito telefonico e indirizzo e-mail);
- Dati biometrici (caratteristiche fisiche, fisiologiche o comportamentali raccolte tramite foto/video riconoscimento);
- Dati di navigazione e Log (IP, dati relativi alla connessione, nomi a dominio ed altri parametri relativi al sistema operativo e al browser e da te utilizzato).

8.4.3 Finalità del trattamento

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al Richiedente durante le fasi di richiesta del certificato. L'informativa è anche pubblicata su https://www.namirial.com/it/documentazione/ , nella sezione specifica Informativa privacy.

Di seguito, elencate, le finalità del trattamento.

- Fornitura del servizio: i dati vengono raccolti tramite un contratto appropriato e vengono trattati al fine di erogare i servizi elettronici richiesti dagli utenti, in base a quanto descritto nel presente documento;
- Conclusione del contratto e fruizione dei servizi:
- Accertamento dell'identità dell'interessato tramite foto/video riconoscimento
- Consenso; Gestione e riscontro alle richieste di assistenza tecnica, anche online Adempimento ad obblighi di legge, regolamentari nazionali o comunitari
- Invio di informazioni a contenuto informativo
- Analisi statistiche, di business e di mercato, realizzate in forma assolutamente anonima e aggregata
- Tutela giurisdizionale dei diritti Namirial
- Prevenzione delle attività fraudolente tramite l'esecuzione di un controllo dell'affidabilità dei dati forniti dall'interessato in occasione del riconoscimento

8.4.3.1 Informativa sulla privacy e consenso

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al Richiedente durante le fasi di richiesta del certificato. L'informativa è anche pubblicata su https://www.namirial.com/it/documentazione/ , nella sezione specifica Informativa privacy.
L'informativa privacy viene presentata al Richiedente prima dell'avvio della sessione di identificazione. Il meccanismo di acquisizione del consenso esplicito al trattamento dei dati biometrici ai sensi dell'articolo 9 del Regolamento (UE) 2016/679 (GDPR), nonché le modalità di registrazione dello stesso all'interno dell'audit trail, sono disciplinati nell'Addendum Prtner.

8.4.4 Modalità del trattamento

Tutte le informazioni personali, acquisite durante l'erogazione dei servizi, vengono trattate da Namirial in conformità al GDPR, adottando le opportune misure di sicurezza descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.

I dati in formato elettronico vengono conservati in appositi data server adibiti allo scopo e su supporti ottici all'interno di armadi protetti. Namirial S.p.A. si riserva l'opportunità di conservare i dati cartacei presso la propria sede centrale, all'interno di archivi cartacei protetti cui hanno accesso solo gli incaricati espressamente autorizzati

8.4.5 Altre forme di utilizzo dei dati

I dati personali possono essere usati con finalità diverse rispetto alla fornitura dei servizi descritti dal presente manuale e possono essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, qualora gli stessi soggetti ne facciano richiesta per motivi di ordine pubblico e nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, la prevenzione, l'accertamento e/o la repressione dei reati.

Maggiori informazioni sono consultabili all'indirizzo https://www.namirial.com/it/privacy-policy

8.4.6 Conservazione dei dati

Le evidenze della verifica dell'identità sono conservate da Namirial per il periodo concordato con il Partner e specificato nell'Addendum. Qualora la sessione NOB si concluda con l'emissione di un certificato qualificato, le evidenze vengono conservate per almeno 20 (venti) anni dalla data di emissione, indipendentemente da quanto indicato nell'Addendum.

8.4.7 Trasferimento dei dati

I dati personali non verranno trasferiti a terzi, salvo nei seguenti casi:

- quando richiesto dalla normativa applicabile;
- in presenza di un legittimo interesse;
- per ottemperare a una richiesta dell'autorità giudiziaria o amministrativa competente;
- in caso di cessazione del servizio.

Namirial non effettua trasferimenti internazionali di dati al di fuori dell'UE o del SEE. I trasferimenti successivi da parte del Partner a terzi sono soggetti agli obblighi di protezione dei dati del Partner stesso.

8.5 Diritti di Proprietà Intellettuale

Il presente documento è di proprietà di Namirial S.p.A., che si riserva tutti i diritti. Per quanto concerne la titolarità di altri dati e informazioni, si applica la normativa vigente.

8.6 Obblighi, garanzie e responsabilità

8.6.1 Obblighi dell'IPSP

Namirial, in qualità di IPSP, è tenuta a:

- operare in conformità con il presente Manuale Operativo e alla normativa applicabile, nonché lo standard ETSI TS 119 461;
- rispettare i requisiti della normativa applicabile in materia di verifica dell'identità;
- identificare con certezza il Richiedente che si sottopone all'onboarding;
- verificare l'autenticità della richiesta di onboarding;
- emettere e gestire le evidenze della verifica dell'identità;
- registrare e conservare le evidenze relative a ciascuna verifica dell'identità, con data e ora certificate da un riferimento temporale qualificato;
- conservare elettronicamente tutte le evidenze per i periodi specificati nel presente documento;
- fornire una copia del presente Manuale Operativo a chiunque ne faccia richiesta;
- adottare misure sicure per il trattamento dei dati personali in conformità con il GDPR;
- rispettare tutti gli obblighi derivanti dal Contratto per il Trattamento dei Dati stipulato con il Partner.

8.6.2 Obblighi dei Richiedenti

In tutti i casi, il richiedente è tenuto a:

- fornire tutte le informazioni richieste e garantirne la veridicità e affidabilità;
- fornire, con consenso esplicito, la raccolta dei dati richiesti per l'identificazione;

- presentare un documento d'identità valido che soddisfi i requisiti indicati nel presente documento;
- non tentare di aggirare o compromettere il processo di identificazione;
- notificare tempestivamente qualsiasi variazione delle informazioni e delle circostanze dichiarate in fase di identificazione.

8.6.3 Obblighi del Relying Party

Il relying party che utilizza le evidenze di verifica dell'identità NOB è tenuto a:

- assicurarsi che l'IPSP o il TSP sia certificato o dimostri la conformità alla ETSI TS 119 46;
- assicurarsi che le evidenze di verifica dell'identità o gli attributi di identità provengano da una fonte attendibile e affidabile;
- definire in modo chiaro le aspettative e le modalità di utilizzo dei dati verificati;
- astenersi dall'utilizzare il servizio per finalità illecite o comunque in contrasto con le disposizioni contrattuali applicabili;
- mantenere costantemente aggiornate e adeguate tutte le risorse necessarie per il corretto utilizzo del servizio.

Ulteriori obblighi del relying party sono definiti nello specifico Addendum, Sezione C.

8.6.4 Garanzie del IPSP

L'IPSP garantisce che il processo di identity proofing è eseguito in conformità ai requisiti applicabili della ETSI TS 119 461 e alle normative vigenti, assicurando l'adozione di misure tecniche e organizzative adeguate alla corretta verifica e il binding dell'identità del Richiedente. L'IPSP garantisce inoltre la tracciabilità delle operazioni effettuate e la conservazione delle evidenze necessarie a supportare il livello di assurance dichiarato per il processo di identificazione.

8.6.5 Garanzie della relying party

La Relying Party garantisce di utilizzare le informazioni e gli attributi di identità ricevuti esclusivamente per le finalità consentite e nel rispetto delle condizioni di utilizzo applicabili e della normativa vigente. La Relying Party garantisce inoltre di effettuare le verifiche necessarie per valutare l'affidabilità dei dati ricevuti, conformemente al livello di assurance dichiarato e alle regole di validazione applicabili, assumendosi la responsabilità delle decisioni basate su tali informazioni.

8.6.6 Garanzie del Richiedente

Il Richiedente garantisce che tutte le informazioni, i dati e i documenti forniti nell'ambito del processo di identificazione sono veritieri, completi, accurati e aggiornati. Il Richiedente garantisce inoltre di essere legittimato a richiedere l'attivazione del servizio

e l'emissione degli eventuali certificati o credenziali associate, nonché di utilizzare il servizio nel rispetto della normativa applicabile e delle condizioni contrattuali.

8.6.7 Responsabilità del Richiedente

Il Richiedente è responsabile della correttezza, completezza e aggiornamento delle informazioni e dei dati forniti nell'ambito del processo di identity proofing.
Il Richiedente è responsabile di tutte le azioni effettuate tramite le proprie credenziali o strumenti di autenticazione, salvo i casi di utilizzo non autorizzato non imputabili a negligenza o dolo.
Il Richiedente è altresì responsabile della tempestiva comunicazione di qualsiasi evento che possa compromettere la sicurezza del processo di identificazione o la validità dell'identità verificata.

8.6.8 Esclusione di garanzie

Salvo quanto previsto dalla normativa applicabile, dalle Condizioni di Contratto e dal presente documento, Namirial non presta ulteriori garanzie rispetto a quelle espressamente indicate nei documenti contrattuali.

8.6.9 Limitazione di responsabilità

Namirial non è responsabile per ritardi, errori o inadempimenti imputabili a terzi, né per anomalie nell'erogazione del servizio che esulino dal proprio controllo tecnico, inclusi, a titolo esemplificativo, malfunzionamenti delle reti di telecomunicazione o telematiche.

Namirial non è altresì responsabile per:

- informazioni errate, incomplete o false fornite dal Richiedente;
- uso improprio del servizio da parte del Partner o dei relativi Richiedenti;
- decisioni adottate dal Partner o da terzi esclusivamente sulla base dell'esito del processo di verifica dell'identità;
- indisponibilità del servizio dovuta a attività di manutenzione programmata o a malfunzionamenti tecnici imprevisti.

La responsabilità di Namirial è limitata ai soli casi in cui sia dimostrabile una violazione sostanziale imputabile a dolo o colpa grave.

Namirial non è responsabile per danni indiretti, consequenziali, perdita di profitto, perdita di dati o altri danni non direttamente imputabili a un inadempimento della stessa.

Resta ferma la responsabilità per gli obblighi inderogabili previsti dalla normativa applicabile, inclusa la normativa in materia di servizi fiduciari e protezione dei dati personali.

8.6.10 Allocazione delle responsabilità e indennizzi

L'allocazione delle responsabilità tra Namirial e il Partner — inclusi i limiti di copertura assicurativa applicabili nel rapporto *B2B* e gli eventuali obblighi di indennizzo è disciplinata esclusivamente dall'Addendum Partner.

8.7 Indennizzi e limitazioni di indennizzo

Namirial è manlevata e tenuta indenne da qualsiasi pretesa, danno, perdita o costo (incluse ragionevoli spese legali) derivante da violazioni di obblighi contrattuali o normativi non imputabili a Namirial, inclusi l'uso non conforme del servizio o la fornitura di informazioni inesatte, incomplete o non aggiornate. L'obbligo di indennizzo non si applica nella misura in cui il danno sia causato da dolo o colpa grave imputabile a Namirial.

8.8 Termini e risoluzione

Le disposizioni del presente documento si applicano dalla data di adesione da parte dell'utente al servizio di Onboarding, messo a disposizione da Namirial, e si intendono integralmente accettate.

8.9 Procedure di risoluzione delle controversie

Eventuali reclami o segnalazioni possono essere presentati attraverso gli appositi canali messi a disposizione da Namirial, secondo le modalità previste dalla procedura interna di gestione dei reclami.

Namirial assicura la presa in carico tempestiva dei reclami ricevuti e la loro gestione secondo criteri di tracciabilità, trasparenza e correttezza, fornendo riscontro entro i termini previsti dalla procedura applicabile

8.10 Termini e Condizioni

I Termini e le Condizioni presentati ai richiedenti prima dell'avvio della sessione NOB e il meccanismo con cui viene registrata l'accettazione sono definiti nell'Addendum partner.

I Termini e le Condizioni di Namirial disciplinano esclusivamente il rapporto commerciale *B2B* tra Namirial e il Partner, come definito nell'accordo commerciale.

8.11 Foro competente

Per tutte le controversie nascenti dal presente Manuale Operativo, dai Termini e Condizioni accettati dal Richiedente o da ulteriori eventuali contratti stipulati per la fruizione dei servizi messi a disposizione da Namirial sarà competente esclusivamente il foro di Ancona.

8.12 Legge applicabile

L'erogazione del servizio e la stipula dei contratti sono soggetti alla Legge Italiana e come tale saranno interpretati ed eseguiti. Il servizio è erogato in conformità alla legge italiana, al Regolamento eIDAS e allo standard ETSI TS 119 461.