

IG PERSONA

documento funzionale

Revision 1.2 - 26 April 2026

COPYRIGHT DISCLAIMER

Tutti i Contenuti (testi, immagini, specifiche tecniche e altro) del presente documento sono **proprietà esclusiva e riservata di Intesi Group** e/o dei suoi aventi causa e/o di terzi soggetti ove indicati, e sono protetti dalle vigenti norme nazionali ed internazionali in materia di proprietà Intellettuale e/o Industriale.

É pertanto vietato utilizzare in qualsiasi modalità (a mero titolo esemplificativo, modificare, copiare, riprodurre, distribuire, trasmettere o diffondere) i suddetti Contenuti senza la previa autorizzazione scritta da parte del Titolare e/o dagli aventi diritto che se ne riservano espressamente ogni forma di riproduzione ed utilizzo. Ogni violazione sarà perseguita a norma di legge.

All Contents (texts, images, technical specifications and more) of this document are the **exclusive and reserved property of Intesi Group** and/or its successors in title and/or third parties where indicated, and are protected by current national and international regulations in intellectual and/or industrial property matters.

It is therefore forbidden to use in any way (by way of example only, modify, copy, reproduce, distribute, transmit or disseminate) the aforementioned Contents without the prior written authorization of the Owner and/or those entitled who expressly reserve any form of reproduction and use it. Any violation will be prosecuted according to the law.

History

Revision	Date	Author	Description
1.0	10/04/2026	A.Dondoni	Prima stesura
1.1	16/04/2026	A.Dondoni	Aggiornamento scenari di utilizzo
1.2	26/04/2026	A.Dondoni	Gestione identificativo nazionale

Index

1. Introduzione	4
2. Overview	5
3. Architettura logica	6
4. IG PERSONA Selfie/Video	8
4.1. Flusso di identificazione	8
4.2. Avvio onboarding	10
4.3. Acquisizione documento di identificazione	10
4.4. Verifica presenza fisica (liveness)	11
4.5. Video con interazione vocale	12
4.6. Review e completamento del processo	13
4.7. Identificativo nazionale	14
4.8. Operatore back office	16
5. Scenari di utilizzo di IG PERSONA	17
5.1. LoIP Substantial – Advanced Signature	18
5.2. LoIP Extended	20
6. Calcolo dello score e validazione del processo	23
6.1. Antifraud Veridas	23
7. Overview tecnologia VeriDas	27
7.1. Validazione del documento di identità	27
7.2. Controlli di sicurezza sul documento	27
7.3. Verifica biometrica	28
7.4. Liveness detection	29
7.5. Rilevamento degli injection attack	30
8. Gestione degli errori nel processo di identificazione	32
8.1. Errori nella scansione del documento	32
8.2. Errori nella fase Selfie	32
8.3. Errori nella fase Video	34

1. Introduzione

IG PERSONA è la soluzione sviluppata da Intesi Group per garantire la sicurezza e l'affidabilità dei processi di identificazione, in conformità ai requisiti della norma ETSI TS 119 461, come richiesto dal Regolamento UE 2024/1183 (eIDAS2) e dal Regolamento di esecuzione della Commissione (UE) 2025/1566.

2. Overview

IG PERSONA è una soluzione completa e flessibile per orchestrare i percorsi di onboarding digitale, progettata per garantire la massima conformità normativa, un elevato livello di sicurezza e un'esperienza utente semplice e guidata.

La piattaforma consente di gestire più metodi di identificazione da un unico punto di integrazione, riducendo la complessità tecnica e operativa e assicurando al contempo un processo di identificazione affidabile e orientato alla qualità del dato.

Basata su un'architettura modulare, **IG PERSONA** è predisposta per integrare le future evoluzioni dell'identità digitale, come l'EUDI Wallet, e in roadmap per la Certificazione **ETSI TS 119 461 v2.1.1**.



Nel momento della stesura del documento, la soluzione integra le modalità di identificazione IG PERSONA **Selfie** e IG PERSONA **Video**.

3. Architettura logica

Di seguito lo schema logico della soluzione **IG PERSONA**, che illustra le integrazioni con le componenti esterne e il flusso del processo di identificazione.

Il diagramma mostra la componente **XpressID**, integrata all'interno del layer di presentazione di **IG PERSONA**. La componente tecnologica di **VeriDas** offre il servizio di verifica dell'identità attraverso la comunicazione con i propri servizi cloud proprietari.

XpressID, attivata a partire dal momento in cui viene visualizzato il QR Code, gestisce l'intera fase di acquisizione del documento, fino all'esecuzione del selfie e del video per i controlli biometrici.

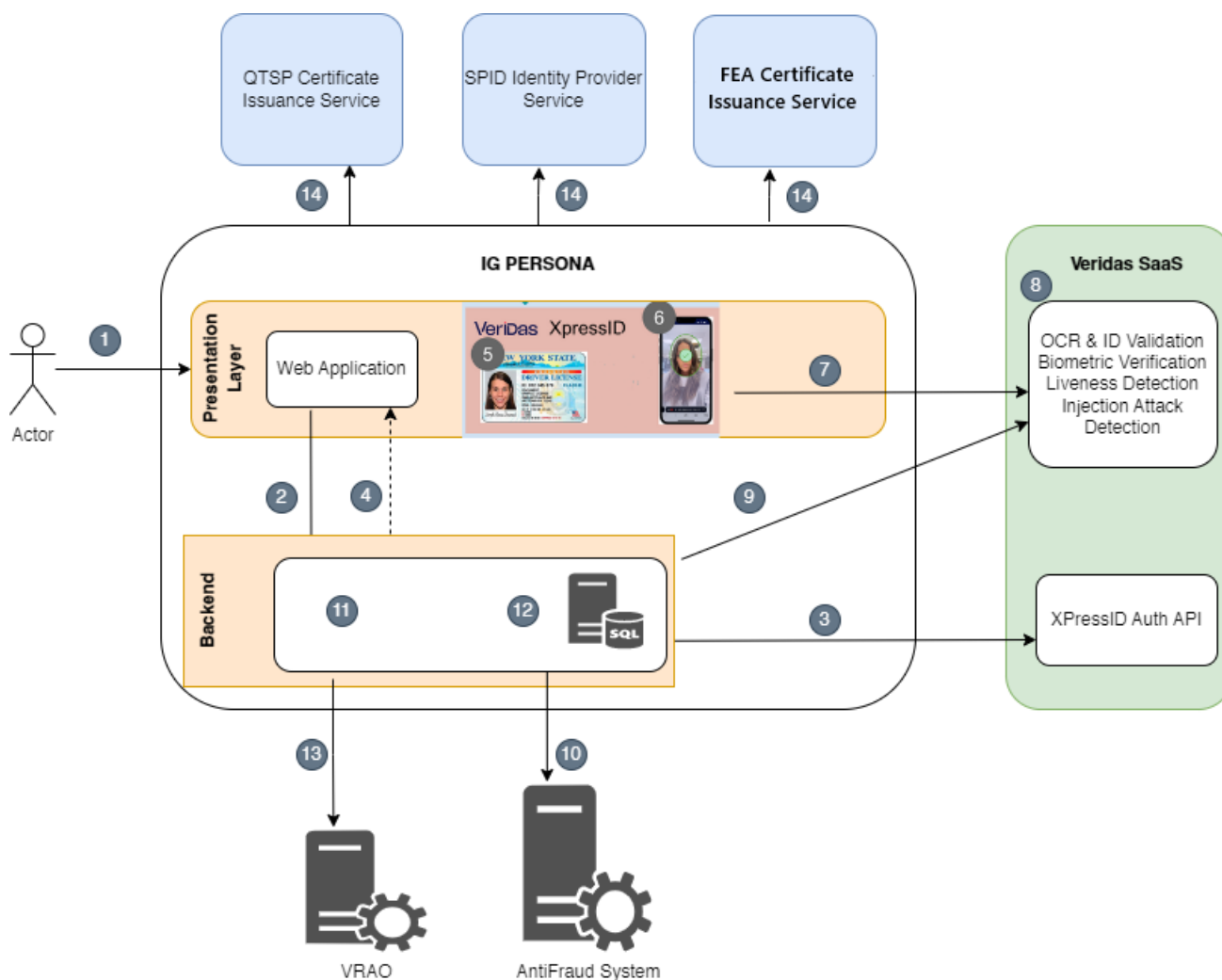


Figure 1. Architettura logica e flusso

IG PERSONA interagisce con i seguenti sistemi esterni:

QTSP Certificate Issuance Service

Gestione del servizio di emissione dei certificati qualificati.

FEA Certificate Issuance Service

Gestione del servizio di emissione dei certificati FEA.

SPID Identity Provider

Servizio di identità digitale eID notificato in ambito italiano.

VRAO

Archiviazione delle evidenze generate nel corso del processo di identificazione.

Antifraud System

Sistema antifrode sviluppato da Intesi Group e integrato nel flusso di identificazione.

4. IG PERSONA Selfie/Video

IG PERSONA, nelle modalità **Selfie** e **Video**, è la soluzione sviluppata da **Intesi Group** che consente al cliente di completare in autonomia la procedura di identificazione.

Il processo può essere eseguito interamente da smartphone oppure in modalità ibrida, avviando la sessione da desktop e completando l'acquisizione delle evidenze tramite smartphone, in modo semplice e intuitivo.

L'intera procedura è guidata da istruzioni testuali e visive, che accompagnano l'utente passo dopo passo fino al completamento del processo.

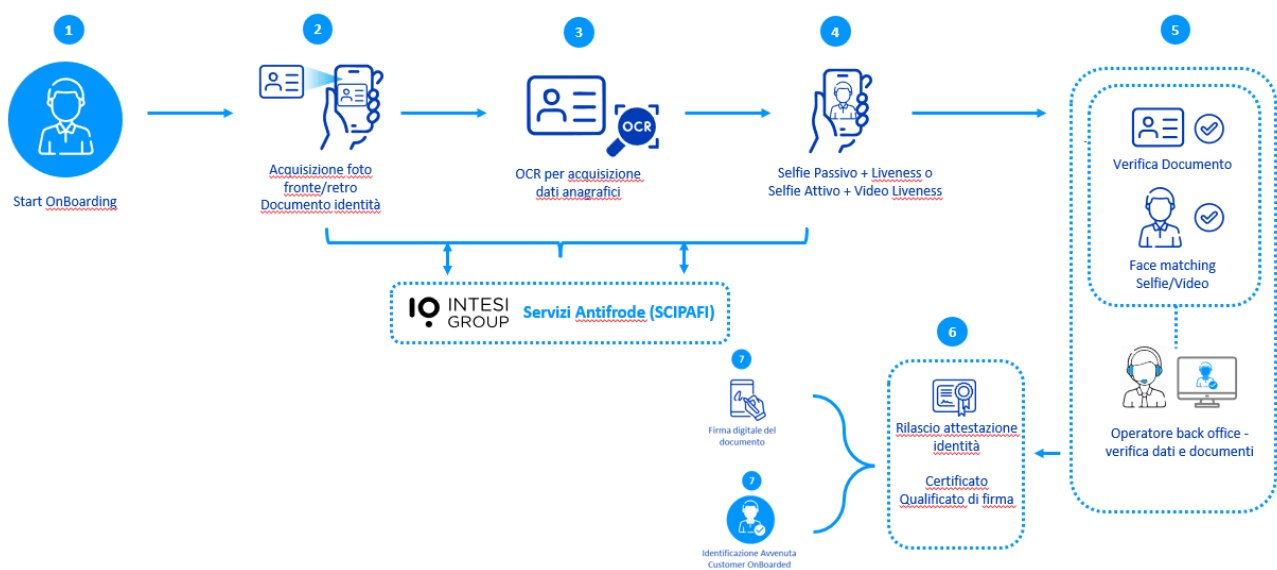


Figure 2. User Journey

4.1. Flusso di identificazione

1. L'utente accede all'applicazione web **IG PERSONA** per avviare il processo di onboarding e accetta i termini e le condizioni del servizio.
2. L'applicazione web comunica con il servizio backend per richiedere l'avvio del processo di verifica dell'identità.
3. Il sistema backend richiede un token di accesso univoco al **VeriDas Identity Verification Service** (VeriDas CORE) per l'esecuzione del flusso di onboarding.
4. La componente **XpressID** viene avviata all'interno dell'applicazione web utilizzando il token di accesso ottenuto.
5. L'utente acquisisce il fronte e il retro del documento di identità o del passaporto.
6. L'utente esegue la verifica del liveness (**attivo** o **passivo**), con eventuale acquisizione di un video.
7. La componente **XpressID**, tramite canale sicuro e protetto, invia le evidenze acquisite al **VeriDas**

Identity Verification Service (VeriDas CORE).

8. Il **VeriDas Identity Verification Service** (VeriDas CORE) esegue l'elaborazione delle evidenze acquisite:
 - ◊ Estrazione dei dati OCR dal documento e validazione del documento (**replay attack** | **print attack**).
 - ◊ Confronto biometrico tra la foto stampata sul documento e la foto selfie.
 - ◊ Controllo della presenza fisica (**liveness**).
 - ◊ Verifica degli **injection attack**.
9. Il sistema backend richiama il **VeriDas Identity Verification Service** (VeriDas CORE) per ottenere l'esito del processo di onboarding, inclusi dati OCR, immagini e score di validazione.
10. Il sistema antifrode esegue la valutazione dello scoring e interagisce con eventuali servizi di terze parti integrati nella soluzione, come **Scipafi**.
11. Viene presa una decisione automatica di accettazione o rifiuto del processo.
12. Il sistema backend memorizza le informazioni sull'identità digitale.
13. Il sistema backend archivia le evidenze di identificazione nello storage **VRAO NFS**.
14. Nel caso di un processo sincrono in presenza, il processo validato può proseguire con gli step successivi.

4.2. Avvio onboarding

Il processo ha inizio con l'accesso del cliente alla soluzione **IG PERSONA** tramite un link univoco di identificazione.

Il link può essere ottenuto secondo una delle seguenti modalità:

Via API

Integrazione applicativa per l'avvio programmatico del processo.

Tramite Portale Operatori

Avvio manuale del processo per identificazioni in presenza (**deVisu**).

Via e-mail

Invio del link al cliente per l'esecuzione in modalità remota.

Prima di avviare l'acquisizione del documento, al cliente viene richiesto di confermare o inserire i propri dati personali: nome, cognome, indirizzo e-mail e numero di telefono (cellulare). I dati di contatto vengono verificati tramite apposito codice di verifica, inviato prima via SMS e successivamente via e-mail.

Previa accettazione dell'informativa privacy e del consenso al trattamento dei dati particolari, il cliente può procedere con la verifica dell'identità.

4.3. Acquisizione documento di identificazione

In base alla nazionalità del documento, il cliente seleziona la tipologia con cui intende effettuare il riconoscimento.

Per i **documenti italiani** sono ammessi:

- Carta d'Identità Elettronica (CIE)
- Patente di guida
- Passaporto

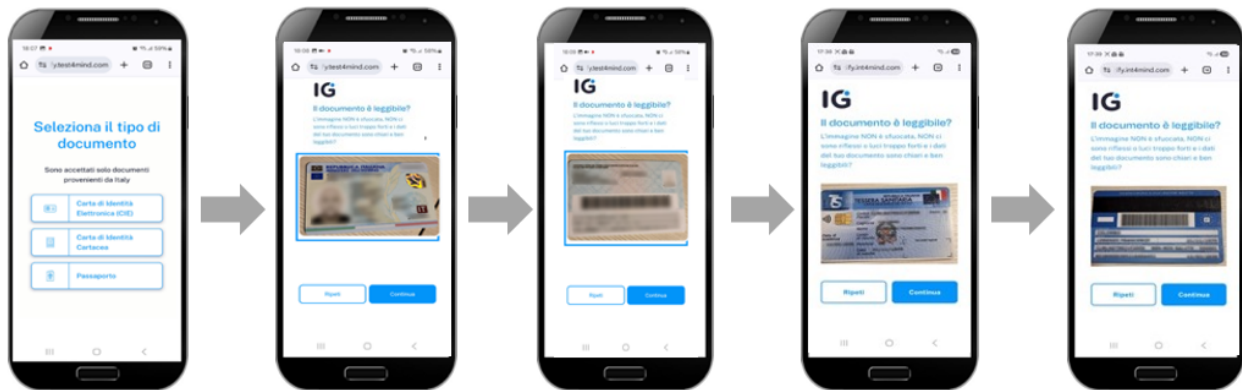


Per i documenti italiani, il processo prevede inoltre l'acquisizione della **Tessera Sanitaria**.

Per i **documenti non italiani** sono ammessi:

- Documento di identità nazionale del paese di origine
- Passaporto

La procedura è guidata da apposite istruzioni che accompagnano il cliente in ogni fase del processo, garantendo un'esperienza semplice e intuitiva.



Selezione. L'utente sceglie il tipo di documento da utilizzare

Cattura Fronte. L'utente viene guidato a centrare il documento per garantire una cattura

Cattura Retro. Il processo viene ripetuto per il retro completando l'acquisizione.

Figure 3. Selezione tipologia documento

Questa fase è gestita dalla componente **XpressID** e il flusso viene interrotto esclusivamente nel caso in cui la tipologia del documento presentato non corrisponda a quella selezionata dal cliente. In tal caso, un apposito messaggio di errore informa l'utente e lo invita a ripetere l'acquisizione ripartendo dalla selezione del tipo di documento.



Non vengono effettuate valutazioni automatiche sulla qualità delle immagini acquisite. Appositi messaggi invitano il cliente a verificare la leggibilità del documento prima di procedere, al fine di garantire una corretta validazione e lettura dei dati in esso contenuti.

4.4. Verifica presenza fisica (liveness)

Il processo di verifica della presenza fisica può essere eseguito secondo due modalità:

- **IG PERSONA Selfie** (modalità passiva): al cliente viene richiesto di acquisire un semplice selfie per il rilevamento del volto.
- **IG PERSONA Video** (modalità attiva): al cliente viene richiesto, oltre al selfie, di eseguire un doppio movimento del capo seguendo le istruzioni fornite dalla procedura a schermo.



La modalità attiva garantisce un livello di verifica della presenza fisica più elevato rispetto alla modalità passiva, in quanto richiede un'interazione dinamica da parte del cliente durante l'acquisizione.



Nella modalità attiva, qualora i movimenti effettuati dal cliente non risultassero coerenti con quelli richiesti, un apposito messaggio di errore lo informa dell'incongruenza.

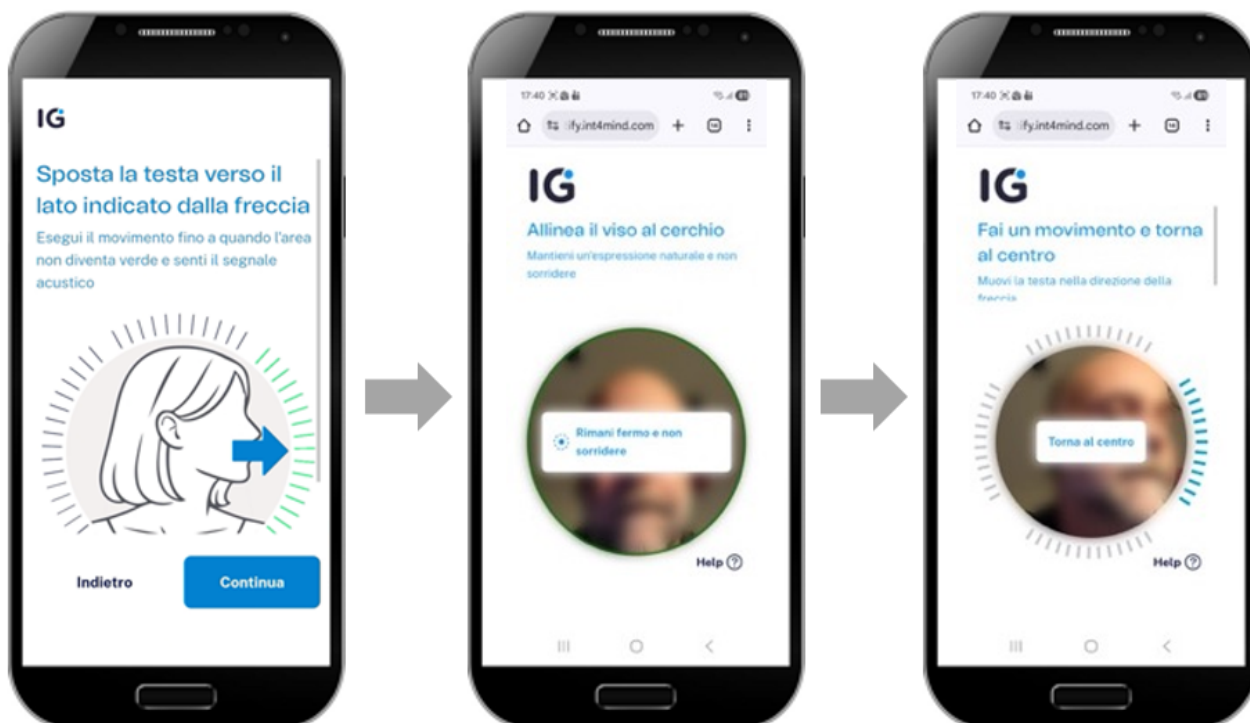


Figure 4. Acquisizione movimento Selfie Attivo

4.5. Video con interazione vocale

Nella sola modalità **IG PERSONA Video**, l'ultimo step prevede l'acquisizione di un breve video nel quale viene chiesto di pronunciare al cliente il proprio nome e cognome e di mostrare il fronte del documento di identificazione — ovvero il lato recante la foto del volto — di fronte alla telecamera.

L'obiettivo di questo step è la **conferma dell'intento**: il cliente non assume un ruolo passivo, ma attraverso un'interazione sia vocale che fisica rafforza la conformità legale dell'intera procedura di identificazione.



In questo step il flusso non prevede interruzioni né messaggi di errore bloccanti. Qualora le condizioni di acquisizione del documento non risultassero ottimali, appositi messaggi guidano il cliente ad adeguare l'inquadratura o le condizioni ambientali, mantenendo il processo in attesa fino al completamento dell'acquisizione.

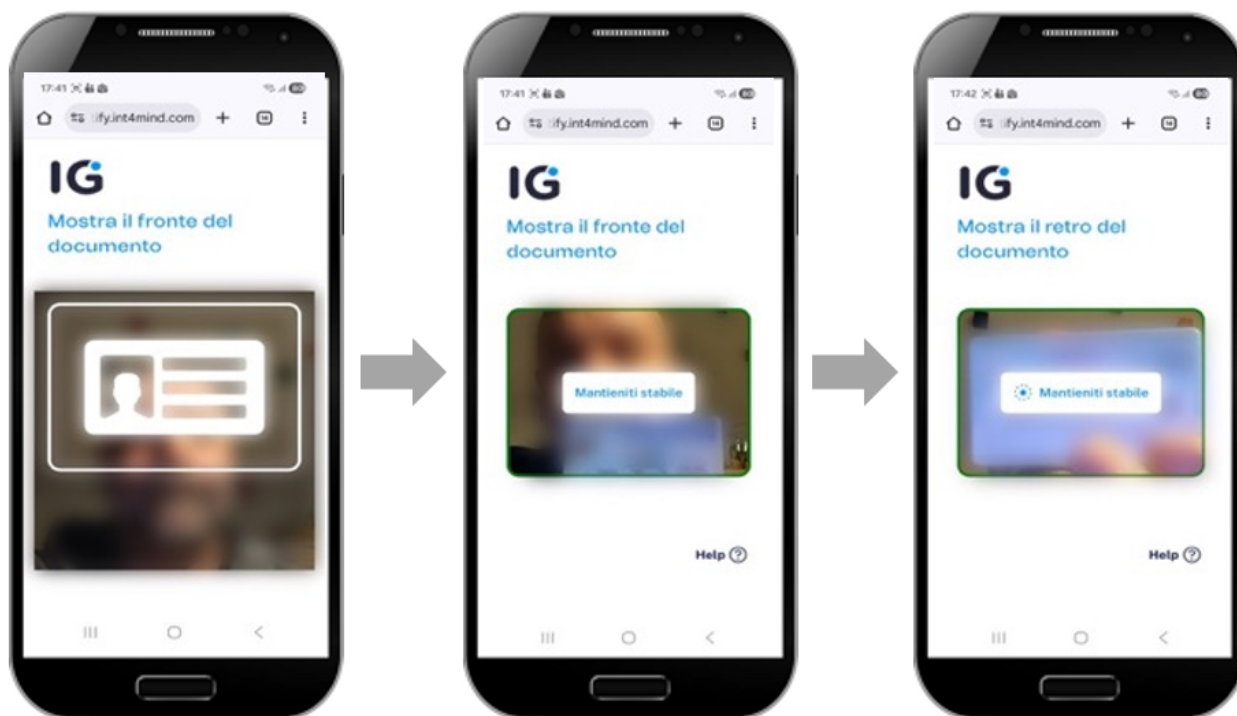


Figure 5. Acquisizione video con documento

4.6. Review e completamento del processo

Completati tutti gli step del processo di verifica dell'identità, il cliente accede a una pagina di riepilogo attraverso la quale può consultare tutte le evidenze e i dati acquisiti nel corso della procedura.

I seguenti dati anagrafici vengono pre-compilati automaticamente sulla base delle informazioni estratte dal documento:

- Nome
- Cognome
- Data di nascita
- Estremi del documento di identificazione



Il cliente mantiene il controllo completo sui propri dati: prima di procedere all'invio finale, ha la possibilità di verificare le informazioni pre-compilate e apportare eventuali correzioni.



Eventuali modifiche apportate dal cliente nella fase di review verranno sottoposte a verifica da parte dell'**Antifraud System**, al fine di rilevare e impedire alterazioni fraudolente dei dati acquisiti.

4.7. Identificativo nazionale

Con il termine **identificativo nazionale** definiamo il codice alfanumerico nazionale che può essere inserito all'interno del certificato di firma qualificata. Per l'Italia, l'identificativo è rappresentato dal **codice fiscale**, mentre per altri Paesi UE può essere il **PNO (Personal Identification Number)**.

L'identificativo nazionale, come mostrato di seguito, viene gestito nella fase di **review** e consente di coprire i seguenti casi:

- Cliente con documento di identificazione italiano che richiede l'inserimento del codice fiscale.
- Cliente con documento di identificazione non italiano che richiede l'inserimento del codice fiscale.
- Cliente con documento di identificazione non italiano che richiede l'inserimento del PNO.

Identificativo Nazionale

* Tipo Identificativo Nazionale:
Codice Fiscale

* Codice fiscale:

* Stato Emissione Codice Fiscale:
Italia [IT]

* Documento richiesto
Nessun file selezionato. [Sfoglia...](#)
[Lista documenti accettati](#)

Figure 6. Identificativo nazionale all'interno della pagina di review

Nel caso di cliente con documento di identificazione italiano che non presenta la **Tessera Sanitaria** durante il processo di verifica dell'identità, la sezione viene mostrata come obbligatoria e, oltre all'inserimento del codice fiscale, viene richiesta l'evidenza tramite caricamento manuale di documenti che ne attestino il valore, quali il certificato di attribuzione del codice fiscale o il certificato AIRE che ne riporti il valore.

Nel caso di cliente con documento di identificazione NON italiano, potrà richiedere l'inserimento del codice fiscale all'interno del certificato qualificato di firma digitale valorizzando l'apposita sezione e allegando il documento richiesto.

4.7.1. Gestione verifica dell'identità senza tessera sanitaria (solo per clienti con documento italiano)

Nella modalità **IG PERSONA Video**, qualora il cliente in possesso di un documento di identificazione italiano non sia in possesso della **Tessera Sanitaria**, può selezionare l'apposito checkbox per procedere con la verifica dell'identità.

Dati personali

Verifica la tua identità

Informazioni importanti

- Inizia**
* Selezionare il paese del documento di identificazione
Italia [IT]
- Verifica il documento di identità**
Il documento deve essere:
 - valido e non scaduto
 - originale, non sono ammesse copie
 - foto ben visibile del titolare
- Effettua un selfie**
Cattura il tuo viso ed effettua dei movimenti seguendo le istruzioni fornite
- Effettua un video**
Cattura il tuo viso, pronuncia il tuo nome e cognome e a seguire mostra il documento di fronte alla fotocamera

☒ Non sono in possesso della Tessera Sanitaria

Continua

Figure 7. Verifica dell'identità senza tessera sanitaria

A fronte della selezione, viene mostrato al cliente un messaggio informativo che lo avvisa della necessità di integrare l'inserimento del codice fiscale allegando documenti aggiuntivi a supporto dell'identificativo nazionale.

Info

Se NON sei in possesso della **Tessera Sanitaria**, durante il processo di identificazione ti verrà richiesto di inserire il codice fiscale e caricare uno dei seguenti documenti.

- Certificato di attribuzione del codice fiscale ?
- Certificato AIRE - solo se riporta il codice fiscale ?

CHIUDI

Figure 8. Verifica dell'identità senza tessera sanitaria

Come descritto in precedenza, in fase di review il cliente dovrà completare il processo inserendo il codice fiscale e caricando il documento richiesto.

Sarà poi compito dell'operatore di back office verificare le evidenze documentali acquisite per procedere con l'approvazione del processo di identificazione.

4.8. Operatore back office

L'operatore di back office, negli scenari che lo prevedono, interviene per validare i dati e le evidenze acquisite durante il processo di identificazione.

Nella modalità **IG PERSONA Video**, il processo di identificazione prevede sempre la validazione da parte dell'operatore.

Nella modalità **IG PERSONA Selfie**, l'operatore interviene in base allo scenario previsto, come descritto nel capitolo successivo.

Il processo di validazione viene sempre eseguito tramite il **Portale RAO (PkRA)**; come riportato nelle [release note](#) del prodotto, una dashboard dedicata, corredata di evidenze e score, consente all'operatore di effettuare una valutazione più oggettiva e accurata.

5. Scenari di utilizzo di IG PERSONA

Il processo di identificazione tramite **IG PERSONA** consente di raggiungere un livello di identificazione **extended**, requisito obbligatorio per l'erogazione di servizi qualificati ai sensi del nuovo Regolamento **eIDAS 2**. Con criteri meno restrittivi, la soluzione può essere adottata anche per quei servizi per i quali è sufficiente un livello di identificazione **substantial**.

Il processo può essere eseguito secondo due modalità di identificazione:

Modalità DeVisu

Il processo viene avviato direttamente dall'operatore incaricato del riconoscimento (RAO), che guida e assiste il cliente durante l'esecuzione della procedura in presenza fisica.

Modalità Remota

Il cliente, partendo dal link di avvio processo, esegue autonomamente il processo di identificazione; l'operatore interviene successivamente per verificare le evidenze e i dati acquisiti nel corso della procedura.

Di seguito riportiamo il riepilogo degli scenari supportati dai processi di identificazione IG PERSONA **Selfie** o **Video**:

Livello (LoIP)	Servizio	Scenario IG PERSONA	Modalità identificazione	Evidenze richieste
Substantial	Advanced Signature	SELFIE	Remota	Fronte/Retro Documento + Selfie + Liveness Passivo
		SELFIE AUTO_APPROVE	Remota	Fronte/Retro Documento + Selfie + Liveness Passivo
		SELFIE AUTO_ENROLL	Remota	Fronte/Retro Documento + Selfie + Liveness Passivo

Livello (LoIP)	Servizio	Scenario IG PERSONA	Modalità identificazione	Evidenze richieste
Extended	Qualified Signature – Smart Card	SELFIE	DeVisu	Fronte/Retro Documento + Selfie + Liveness Passivo
	Qualified Signature – Remota	SELFIE	DeVisu	Fronte/Retro Documento + Selfie + Liveness Passivo
	SPID – Identità Digitale	SELFIE	DeVisu	Fronte/Retro Documento + Liveness Passivo
	Qualified Signature – Remota	VIDEO	Remota	Fronte/Retro Documento + Liveness Attivo + Video
	SPID – Identità Digitale	VIDEO	Remota	Fronte/Retro Documento + Liveness Attivo + Video
	Sigillo Qualificato	VIDEO	Remota	Fronte/Retro Documento + Liveness Attivo + Video



I documenti supportati variano in base alla nazionalità del cliente. Per i cittadini italiani è generalmente richiesta anche la **Tessera Sanitaria** nei processi a livello **Extended**.

5.1. LoIP Substantial – Advanced Signature

5.1.1. SELFIE | Modalità remota

Il cliente riceve una mail contenente il link per avviare il processo di identificazione tramite **IG PERSONA SELFIE**.

Evidenze acquisite

F/R Documento di riconoscimento + Selfie + Liveness Passivo

Operatore back office

Sempre previsto; verifica le evidenze acquisite, visualizza gli score e approva o rifiuta l'identificazione. In caso di rifiuto, il cliente riceve una nuova mail per ripetere il processo di identificazione.

Rilascio del servizio

Al termine dell'approvazione da parte dell'operatore di back office, il cliente riceve la mail per procedere con l'emissione del certificato.

Documenti supportati

- Esteri: Carta d'identità / Patente / Passaporto
- Italia: CIE / Carta d'identità cartacea / Patente / Passaporto

5.1.2. SELFIE AUTO_APPROVE | Modalità remota

Il cliente riceve una mail contenente il link per avviare il processo di identificazione tramite **IG PERSONA SELFIE**.

Evidenze acquisite

F/R Documento di riconoscimento + Selfie + Liveness Passivo

Operatore back office

Il sistema **ANTI-FRAUD** verifica in modo sincrono i dati acquisiti. Se la verifica è superata, l'operatore non interviene e il cliente riceve direttamente la mail per l'emissione del certificato. In caso contrario, l'operatore di back office interviene per validare i dati.

Rilascio del servizio

Il cliente riceve la mail per procedere con l'emissione del certificato.

Documenti supportati

- Esteri: Carta d'identità / Patente / Passaporto
- Italia: CIE / Carta d'identità cartacea / Patente / Passaporto

5.1.3. SELFIE AUTO_ENROLL | Modalità remota

Il cliente riceve una mail contenente il link per avviare il processo di identificazione tramite **IG PERSONA SELFIE**.

Evidenze acquisite

F/R Documento di riconoscimento + Selfie + Liveness Passivo

Operatore back office

Il sistema **ANTI-FRAUD** verifica in modo sincrono i dati acquisiti. Se la verifica è superata, l'operatore non interviene; e il cliente riceve direttamente la mail che conferma l'avvenuta emissione di un certificato. In caso contrario, l'operatore di back office interviene per validare i dati.

Rilascio del servizio

Il cliente riceve la mail di **conferma emissione** del certificato.

Documenti supportati

- Esteri: Carta d'identità / Patente / Passaporto
- Italia: CIE / Carta d'identità cartacea / Patente / Passaporto



Questa modalità di identificazione supporta solo l'emissione di certificati con OTP via SMS o email.

5.2. LoIP Extended

5.2.1. Firma Qualificata – Smart Card | SELFIE | Modalità deVisu

L'operatore RAO abilitato avvia e conduce il riconoscimento **DE VISU** tramite **IG PERSONA SELFIE**, in presenza fisica del cliente.

Evidenze acquisite

F/R Documento di riconoscimento + F/R Tessera Sanitaria (cittadini italiani) + Selfie Passivo

Verifica identità

Il sistema **ANTI-FRAUD** verifica in modo sincrono i dati acquisiti (max **2 retry**). Se la verifica è superata, l'operatore può procedere con l'approvazione. In caso contrario, il processo viene sospeso in attesa di validazione da parte dell'operatore **SUPERVISORE**, che riceve una mail di ingaggio per approvare o rifiutare l'identificazione.

Al termine, della valutazione del **SUPERVISORE**, l'operatore RAO viene notificato via mail per riprendere il processo e approvare l'identificazione.

Rilascio del servizio

Emissione del certificato su **Smart Card**, direttamente dall'operatore tramite **IG DESK**.

Documenti supportati

- Esteri: Carta d'identità / Passaporto
- Italia: CIE / Patente / Passaporto + Tessera Sanitaria

5.2.2. Firma Qualificata – Remota | SELFIE | Modalità deVisu

L'operatore RAO abilitato avvia e conduce il riconoscimento **DE VISU** tramite **IG PERSONA SELFIE**, in presenza fisica del cliente.

Evidenze acquisite

F/R Documento di riconoscimento + F/R Tessera Sanitaria (cittadini italiani) + Selfie Passivo

Verifica identità

Il sistema **ANTI-FRAUD** verifica in modo sincrono i dati acquisiti (max **2 retry**). Se la verifica è superata, l'operatore può procedere con l'approvazione. In caso contrario, il processo viene sospeso in attesa di validazione da parte dell'operatore **SUPERVISORE**, che riceve una mail di ingaggio per approvare o rifiutare l'identificazione.

Al termine, della valutazione del **SUPERVISORE**, l'operatore RAO viene notificato via mail per riprendere il processo e approvare l'identificazione.

Rilascio del servizio

Il cliente riceve una mail per procedere con l'emissione del certificato di **firma elettronica qualificata**.

Documenti supportati

- Esteri: Carta d'identità / Passaporto
- Italia: CIE / Patente / Passaporto + Tessera Sanitaria

5.2.3. Firma Qualificata – Remota | VIDEO | Modalità remota

Il cliente riceve una mail contenente il link per avviare il processo di identificazione tramite **IG PERSONA VIDEO**.

Evidenze acquisite

F/R Documento di riconoscimento + F/R Tessera Sanitaria (cittadini italiani) + Selfie attivo + Video

Operatore back office

L'operatore verifica le evidenze acquisite, visualizza gli score e approva o rifiuta l'identificazione. In caso di rifiuto, il cliente riceve una nuova mail per ripetere il processo.

Rilascio del servizio

Il cliente riceve una mail per procedere con l'emissione del certificato di **firma elettronica qualificata**.

Documenti supportati

- Esteri: Carta d'identità / Passaporto
- Italia: CIE / Patente / Passaporto + Tessera Sanitaria

5.2.4. SPID – Identità Digitale | VIDEO | Modalità remota

Il cliente riceve una mail contenente il link per avviare il processo di identificazione tramite **IG PERSONA VIDEO**.

Evidenze acquisite

F/R Documento di riconoscimento + F/R Tessera Sanitaria + Selfie attivo + Video

Operatore back office

L'operatore verifica le evidenze acquisite, visualizza gli score e approva o rifiuta l'identificazione. In caso di rifiuto, il cliente riceve una nuova mail per ripetere il processo.

Rilascio del servizio

Il cliente riceve una mail per procedere con l'emissione della **pratica SPID**.

Documenti supportati

- Solo Italia: CIE / Patente / Passaporto + Tessera Sanitaria

6. Calcolo dello score e validazione del processo

Il calcolo dello score al fine di validare ogni processo di identificazione viene gestito dalla componente **Antifraud System** sviluppata iteramente da Intesi Group.

Attraverso apposite procedure di controllo e soglie di guardia, il sistema implementa le seguenti modalità:

- **Antifraud Lite:** processo di valutazione della conformità e formalismo dei dati, univocità delle informazioni di contatto per identificativo utente e verifica della presenza in blacklist del codice fiscale italiano;
- **Antifraud Scipafi:** processo di valutazione antifrode tramite interrogazione del sistema Scipafi - solo per identificazione con documenti italiani;
- **Antifraud Veridas:** processo di valutazione degli score acquisiti al termine del processo di verifica identità. Al termine di questa fase, il processo di identificazione potrà completarsi, interrompersi oppure passare alla fase di controllo tramite operatore.
- **Antifraud Completo:** processo di valutazione antifrode che esegue tutti i controlli richiesti

Il processo di score è abilitato sulla base di uno specifico **profilo** abilitante le diverse modalità descritte in precedenza.

Il sistema supporta due tipi di flussi:

Flusso Sincrono

il calcolo del score viene eseguito immediatamente all'interno del processo di identificazione, eseguendo tutti i processi di scoring abilitati.

Flusso Asincrono

il calcolo del score viene differito e gestito tramite un meccanismo basato su eventi.

6.1. Antifraud Veridas

Il processo gestisce gli score generati e restituiti dal servizio di **Digital Onboarding Veridas** al termine dell'analisi del documento di identificazione e della valutazione biometrica.

Score-DocumentGlobal

Score principale per il processo di verifica del documento di identità. Controlla l'autenticità e la validità del documento presentato.

I seguenti score vengono generati e restituiti dal servizio di **Digital Onboarding Veridas** al termine dell'analisi della foto selfie e del video.

ValidasScoreSelfie

Score principale per l'analisi di similarità tra la foto selfie e la foto del volto presente sul documento di identità.

Indica la probabilità che i due volti appartengano alla stessa persona.

ValidasScoreVideo

Indica la probabilità che la foto selfie e il volto rilevato nel video selfie appartengano alla stessa persona.



Questo score è valutato solo nella modalità di identificazione IG PERSONA Video.

ValidasScoreLifeProof

Indica la probabilità che la persona ripresa sia effettivamente in vita (liveness detection).

ValidasScorePhotold

Indica la probabilità che la foto selfie e la foto del volto presente sul documento di identità appartengano alla stessa persona.

ValidasScoreSelfieAuthenticity

Indica la probabilità che la foto selfie sia autentica e non il risultato di un tentativo di spoofing.

Il seguente score viene generato e restituito dal servizio backend di **Digital Onboarding Veridas** per ciascuna immagine acquisita, al termine del controllo di integrità. Tali score garantiscono che le immagini catturate tramite XPressID siano pervenute all'applicazione backend senza aver subito modifiche durante la trasmissione.

ValidasScoreIntegrity

Indica se l'integrità dell'intero processo di validazione è stata soddisfatta o meno. Il valore dipende dai seguenti fattori:

- Lo score di integrità è disponibile **esclusivamente** se almeno una delle immagini è stata acquisita tramite un SDK che supporta la funzionalità di integrità.
- Il valore sarà **1** se **tutte** le immagini caricate presentano uno score di integrità pari a **1**.
- Il valore sarà **0** se **almeno una** delle immagini presenta uno score di integrità pari a **0**

Sulla base di questi score principali, viene calcolato il **ValidationGlobalScore**, che rappresenta l'esito complessivo dell'intero processo di validazione.

Gli score principali hanno un valore decimale (float) compreso tra **0** e **1** e indicano, in modo sintetico, se un determinato processo si è concluso con esito positivo o negativo. Il loro utilizzo semplifica la valutazione del risultato, evitando al cliente di dover analizzare singolarmente un numero crescente di score di dettaglio.

Gli score principali sono i seguenti:

- **Score-DocumentGlobal**
- **ValidasScoreSelfie**
- **ValidasScoreVideo**
- **ValidasScoreLifeProof**
- **ValidasScoreIntegrity**

I valori di tali score possono essere classificati come segue:

Valid (Valido)

Il valore è sufficientemente alto da essere considerato positivo.

Inconclusive (Inconcludente)

Le evidenze richiedono una revisione da parte di un operatore umano per determinarne la validità.

Rejected (Rifiutato)

Il valore è sufficientemente basso da essere considerato non corretto, potenzialmente fraudolento o comunque non idoneo.

La seguente tabella riporta i range di valore corrispondenti a ciascuna classificazione:

Score principale	Valid	Inconclusive	Rejected
Score-DocumentGlobal	> 0.70	$0.50 \leq \text{score} \leq 0.70$	< 0.50
ValidasScoreSelfie	> 0.70	$0.50 \leq \text{score} \leq 0.70$	< 0.50
ValidasScoreVideo	> 0.70	$0.50 \leq \text{score} \leq 0.70$	< 0.50
ValidasScoreLifeProof	> 0.70	$0.50 \leq \text{score} \leq 0.70$	< 0.50
ValidasScoreIntegrity	1	n/a	0



Per **ValidasScoreIntegrity** non è previsto uno stato **Inconclusive**: il valore è sempre binario (**1** = integrità confermata, **0** = integrità non confermata).

Il valore di **ValidationGlobalScore** assume uno dei seguenti tre valori, in base alle condizioni riportate:

Condizione	Valore di ValidationGlobalScore
Tutti gli score Score-DocumentGlobal , ValidasScoreSelfie , ValidasScoreLifeProof , ValidasScoreVideo e ValidasScoreIntegrity sono in stato Valid .	1.0
Uno e uno solo degli score sopra indicati è in stato Inconclusive .	0.5
Almeno uno degli score sopra indicati è in stato Rejected , oppure più di uno è in stato Inconclusive .	0.0

7. Overview tecnologia VeriDas

Andiamo ora nel dettaglio di quelle che sono le tecnologie proprietarie sviluppate dal partner tecnologico VeriDas e integrate all'interno della soluzione IG PERSONA.

7.1. Validazione del documento di identità

Il motore OCR di Veridas è sviluppato interamente in proprio ed è stato appositamente addestrato per la lettura di tutti i campi OCR dei documenti di identità. Al termine dell'acquisizione, il sistema restituisce tutte le informazioni visibili del documento acquisito, sia sul fronte che sul retro, garantendo un'accuratezza superiore al **99%** nella maggior parte dei campi.

Il motore supporta la lettura OCR in qualsiasi lingua e nei seguenti alfabeti: **latino, arabo, cinese e cirillico**, inclusi caratteri speciali.



La qualità della validazione dipende da due fattori principali: il **livello di sicurezza intrinseco del documento** (documenti con maggiori misure di sicurezza offrono una verifica digitale più affidabile) e la **tecnologia di acquisizione utilizzata**.

7.2. Controlli di sicurezza sul documento

Il sistema esegue i seguenti controlli per verificare l'autenticità del documento presentato:

1. **Verifica della data di scadenza e della maggiore età:** il sistema verifica che il documento non sia scaduto e che il titolare sia maggiorenne.
2. **Verifica dei checksum MRZ:** il sistema legge e verifica le cifre di controllo della MRZ (Machine Readable Zone) del documento di identità.
3. **Verifica della coerenza tra dati visivi (VIZ) e MRZ:** il sistema verifica il grado di corrispondenza tra i dati scritti nel documento (VIZ) e i dati riportati nella MRZ.
4. **Rilevamento di fotocopie in bianco e nero.**
5. **Rilevamento di fotocopie a colori:** il sistema è in grado di rilevare la presenza di fotocopie a colori su diversi tipi di supporto (carta da ufficio, carta fotografica, documenti plastificati, polycarbonato, ecc.).
6. **Rilevamento di documenti mostrati su schermo:** il sistema è in grado di rilevare la presenza di diversi tipi di schermi (smartphone, tablet e computer desktop).
7. **Rilevamento di alterazione o sostituzione della foto sul documento:** il sistema individua situazioni in cui una foto è stata sovrapposta alla foto originale del documento.
8. **Rilevamento di documenti generati con intelligenza artificiale (deepfake) e manipolazioni digitali:** il sistema è in grado di rilevare manipolazioni totali o parziali dell'immagine eseguite con programmi come Photoshop, nonché documenti generati artificialmente.

9. **Decodifica di codici bidimensionali (OBR):** il sistema supporta diversi formati (Code 128, Code 39, Barcode, DataMatrix, QR e PDF417) e confronta i dati stampati nel documento (VIZ e MRZ) con quelli codificati nei codici bidimensionali per verificarne la coerenza.

7.3. Verifica biometrica

Veridas offre una tecnologia di biometria facciale all'avanguardia, basata su sistemi di intelligenza artificiale addestrati con reti neurali profonde per il riconoscimento del volto. Il motore biometrico è sviluppato interamente in proprio ed è soggetto a valutazioni continue da parte del **NIST** (National Institute of Standards and Technology), ottenendo regolarmente posizioni di vertice nelle classifiche internazionali.

Il motore consente di effettuare confronti tra due immagini (foto selfie o volti presenti su documenti di identità ufficiali) per determinare se appartengono alla stessa persona. Il sistema analizza l'immagine facciale e la converte in un vettore matematico irreversibile, rendendo impossibile il recupero dell'immagine originale qualora tale vettore venga eliminato, garantendo così la **protezione della privacy dell'utente** in ogni fase del processo.

7.3.1. Accuratezza certificata NIST

Il **NIST** è l'agenzia federale statunitense di riferimento internazionale per la valutazione e la classificazione dei motori biometrici. Secondo il report pubblicato da NIST per **FRTE 1:N** nell'aprile 2023, Veridas ha ottenuto nella categoria Mugshot un tasso di falsi negativi (**FNIR**) pari a **0.0232** per un tasso di falsi positivi (**FPIR**) di **0.001**, su un database di 12 milioni di identità.

7.3.2. Assenza di bias

Il motore biometrico di Veridas **non presenta bias** di natura etnica, di genere o di altra natura. Veridas è attivamente coinvolta nella comunità scientifica sul tema dei bias biometrici e ha collaborato con l'**Universidad Autónoma de Madrid** per la definizione di una nuova metrica per la misurazione del bias nei sistemi biometrici.



I sistemi biometrici offrono una maggiore accuratezza rispetto al riconoscimento facciale effettuato da esseri umani. Studi del 2014 hanno dimostrato che le persone ottengono un'accuratezza del **97,53%** nel riconoscimento facciale, mentre gli algoritmi superano il **99%**. A differenza dei bias umani — che non possono essere misurati né auditati oggettivamente — i bias dei sistemi biometrici sono misurabili e verificabili in modo oggettivo.

7.3.3. Confronto biometrico nel processo di on-boarding

Il motore biometrico di Veridas è in grado di confrontare una foto selfie con la foto ritagliata da un documento di identità, secondo gli standard **ICAO**. Il motore è stato specificamente addestrato per

questo caso d'uso, ottimizzando le prestazioni in presenza delle seguenti condizioni variabili:

- Presenza di riflessi nella zona della foto stampata sul documento.
- Presenza di ologrammi (kinegram) e altri artefatti visivi sulla foto stampata.
- Differenza temporale tra la foto selfie acquisita dall'utente e la foto presente sul documento.
- Variazioni nell'aspetto del volto: presenza di barba, baffi, cambiamenti nell'acconciatura, occhiali, trucco, ecc.



Il processo di confronto biometrico viene eseguito in **meno di un secondo**. Il motore restituisce uno score di similarità facciale con valore compreso tra **0** e **1**: più alto è il valore, maggiore è la probabilità che le due immagini appartengano alla stessa persona. Il cliente può scegliere autonomamente la soglia decisionale e modificarla in qualsiasi momento in base al livello di sicurezza richiesto dal proprio caso d'uso.

7.4. Liveness detection

Veridas dispone di una tecnologia proprietaria di liveness detection per il rilevamento di **presentation attack** e **deepfake**. La soluzione è certificata da **iBeta** secondo lo standard **ISO 30.107** ai livelli 1 e 2, sia per la modalità attiva che passiva, in ambienti nativi e web.



La certificazione di **Livello 2** rappresenta il massimo standard disponibile ed è focalizzata sul rilevamento degli attacchi più sofisticati, superando test condotti con manichini realistici e maschere 3D in resina, lattice e silicone, nonché volti sintetizzati tramite immagini digitali.

7.4.1. Tipologie di attacchi rilevati

Il sistema è in grado di rilevare le seguenti tipologie di attacchi:

- **Attacchi con schermi**: utilizzo di uno schermo per riprodurre l'immagine del volto di un'altra persona davanti alla telecamera del dispositivo dell'attaccante.
- **Attacchi video con schermi**: riproduzioni video in cui viene mostrato il volto della persona da impersonare, che richiedono la piena collaborazione del soggetto da imitare.
- **Attacchi con animazioni 3D**: attacchi in cui il volto della persona viene generato artificialmente e animato tramite software.
- **Attacchi con stampe fotografiche**: utilizzo di una o più stampe di un volto umano in diverse qualità di stampa.
- **Attacchi con maschere stampate**: stampa del volto su carta e ritaglio per costruire una maschera 2D.

- **Maschere fotografiche 3D:** composizione di più fotografie stampate sovrapposte per simulare un effetto tridimensionale.
- **Maschere in lattice:** attacco condotto indossando una maschera in lattice davanti alla telecamera.
- **Attacchi con manichini:** attacco condotto posizionando un manichino davanti alla telecamera.
- **Maschere in gesso:** attacco condotto indossando maschere realizzate in gesso e dipinte in dettaglio.
- **Maschere in plastica rigida:** attacco condotto con una maschera rigida in plastica davanti alla telecamera.
- **Maschere in silicone:** attacco condotto con una maschera in silicone davanti alla telecamera.
- **Maschere trasparenti:** attacco condotto utilizzando una maschera traslucida.

7.4.2. Valutazione NIST PAD

Veridas ha sottoposto il proprio motore alla valutazione **NIST PAD**, che misura la capacità di rilevare tentativi di spoofing su immagini o video, indipendentemente dall'utilizzo di SDK di acquisizione, garantendo condizioni di valutazione uniformi per tutti i produttori.

7.5. Rilevamento degli injection attack

Le frodi di identità possono essere condotte secondo due diverse modalità:

Presentation attack

L'attaccante mostra evidenze false davanti alla telecamera del dispositivo di acquisizione, ad esempio una fotocopia, uno screenshot o qualsiasi altro tentativo di impersonificazione.

Injection attack

L'attaccante introduce evidenze false direttamente nel sistema, senza dover presentare nulla davanti alla telecamera, manipolando il canale di acquisizione o il canale di comunicazione.

7.5.1. Misure di sicurezza contro gli injection attack

Il sistema Veridas implementa le seguenti misure di sicurezza per il rilevamento degli injection attack:

API Security

Veridas dispone di numerosi meccanismi di sicurezza che impediscono l'invocazione non controllata delle API per l'iniezione di contenuti non autorizzati. Tali misure includono l'utilizzo di **api-key**, filtri IP e ulteriori controlli descritti nella sezione Infrastructure and Security.

Rilevamento di telecamere virtuali

Il sistema è in grado di rilevare i casi in cui l'attaccante utilizza una telecamera virtuale (es. **VirtualCam**) per iniettare nel sistema l'immagine di un documento o di un volto come se fosse stata acquisita dalla telecamera reale del dispositivo.

Rilevamento di emulatori e altri elementi non affidabili

Veridas dispone di tecnologia per verificare l'affidabilità del dispositivo dal quale viene eseguito il processo di verifica dell'identità. Il sistema è in grado di rilevare processi eseguiti da dispositivi emulati, macchine virtuali, bot o ambienti di sviluppo attivi, considerati non affidabili per l'esecuzione della verifica.

Rilevamento tramite tecniche di Business Intelligence

Veridas analizza decine di parametri relativi al processo per verificare che questo sia stato eseguito in modo completo, end-to-end dallo stesso dispositivo e senza l'utilizzo di evidenze iniettate direttamente nel sistema.



Le misure di sicurezza descritte sono di natura **logica e non statistica**: il loro rilevamento non è pertanto associato a tassi di falsi positivi o falsi negativi.

8. Gestione degli errori nel processo di identificazione

Di seguito vengono riportati i possibili casi di errore gestiti con opportuni messaggi durante il processo di identificazione.



Nessuno scenario è bloccante per il completamento del processo di identificazione da parte del cliente. La soluzione gestisce gli errori risottomettendo lo step al cliente oppure invitandolo a riavviare il processo dal link di inizio procedura.

8.1. Errori nella scansione del documento

Tipo di errore	Titolo messaggio	Messaggio al cliente
Attivazione fotocamera fallita	Impossibile completare il processo di verifica. Riprova.	Impossibile completare il processo di verifica. Riprova.
Fotocamera non rilevata	Nessuna fotocamera rilevata.	Per continuare la procedura, verifica che il tuo dispositivo sia dotato di fotocamera.
Permessi fotocamera/microfono	Autorizzazioni richieste.	Assicurati di consentire alla pagina l'accesso alla fotocamera e al microfono.
Orientamento dispositivo errato	Ruota il tuo dispositivo.	Per continuare, posiziona il tuo cellulare in posizione verticale.
Cambio orientamento durante processo	Riprovare il processo.	Il processo non è stato completato a causa di un cambiamento imprevisto nell'orientamento del dispositivo.
Verifica documento non riuscita	Verifica non riuscita.	Impossibile completare il processo di verifica del documento. Riprova assicurandoti che il documento sia conforme.

8.2. Errori nella fase Selfie

Tipo di errore	Titolo messaggio	Messaggio al cliente
Attivazione fotocamera fallita	Impossibile attivare la fotocamera.	Qualcosa ha impedito alla fotocamera di avviarsi correttamente. Verifica che non sia in uso da parte di un'altra applicazione e riprova.
Fotocamera non rilevata	Nessuna fotocamera rilevata.	Per continuare la procedura, verifica che il tuo dispositivo sia dotato di fotocamera.
Perdita di focus	Il processo è stato interrotto.	Per motivi di sicurezza, la verifica si è interrotta dopo aver rilevato un cambio di applicazione o scheda. Riavviare il processo per continuare.
Nessun movimento rilevato	Nessun movimento della testa rilevato.	Quando richiesto sullo schermo, muovi la testa verso il lato corrispondente e torna al centro quando viene dato il segnale o quando senti il suono.
Permessi fotocamera/microfono	Autorizzazioni richieste.	Non possiamo accedere alla tua fotocamera o al tuo microfono. Abilita le autorizzazioni dalle impostazioni del tuo dispositivo o del browser per continuare.
Orientamento dispositivo errato	Ruota il tuo dispositivo.	Per continuare, posiziona il cellulare in posizione verticale.
Cambio orientamento durante processo	Riprova il processo.	Il processo non è stato completato a causa di un cambiamento imprevisto nell'orientamento del dispositivo.
Verifica gesto non riuscita	Verifica non riuscita.	Sembra che tu abbia fatto un gesto diverso da quello indicato. Per continuare, segui la freccia con la testa a velocità moderata e torna al centro quando richiesto.

8.3. Errori nella fase Video

Tipo di errore	Titolo messaggio	Messaggio al cliente
Attivazione fotocamera fallita	Impossibile attivare la fotocamera.	Qualcosa ha impedito l'avvio corretto della fotocamera. Controlla che non sia in uso da un'altra applicazione e riprova.
Fotocamera non rilevata	Nessuna fotocamera rilevata.	Verifica che il tuo dispositivo abbia una fotocamera per continuare il processo.
Permessi fotocamera/microfono	Permessi richiesti.	Non riusciamo ad accedere alla tua fotocamera o al microfono. Abilita i permessi dalle impostazioni del tuo dispositivo o browser per continuare la verifica.
Orientamento dispositivo errato	Ruota il tuo dispositivo.	Per continuare, posiziona il cellulare in posizione verticale.
Cambio orientamento durante processo	Limite di tempo superato.	Il processo non è stato completato a causa di un cambio di orientamento imprevisto del dispositivo.