

IG PERSONA

Functional Document

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	First draft
1.1	16/04/2026	A. Dondoni	Update on Use Cases
1.2	26/04/2026	A. Dondoni	National ID Management

Sommario

1. Introduction.....	6
2. Overview.....	6
3. Logical Architecture.....	6
4. IG PERSONA Selfie/Video	8
4.1 Identification process	9
4.2 Onboarding Process.....	10
4.3 Scanning of identification documents.....	11
4.4 Liveness check	12
4.5 Video with voice interaction	13
4.6 Review and completion of the process	14
4.7 National ID.....	15
4.7.1 Identity verification without a health card (only for customers with an Italian ID) 16	
4.8 Backoffice operator	18
5 Use Cases for IG PERSONA	18
5.1 LoIP Substantial – Advanced Signature	20
5.1.1 SELFIE - Remote mode	20
5.1.2 SELFIE AUTO_APPROVE Remote mode.....	21
5.1.3 SELFIE AUTO_ENROLL Remote mode	21
5.2 LoIP Extended	22
5.2.1 Qualified Signature – Smart Card SELFIE In person mode	22
5.2.3 QUALified signature – Remote VIDEO Remote mode.....	23
5.2.4 SPID – Digital Identity VIDEO Remote	23

6. Score calculation and process validation	24
6.1 Antifraud Veridas.....	25
7. Overview of VeriDas Technology	28
7.1 ID Validation	28
7.2 Document security checks.....	28
7.3 Biometric verification	29
7.3.1 NIST-certified accuracy	30
7.3.2 Absence of bias	30
7.3.3 Biometric verification during the onboarding process	31
7.4 Liveness detection	31
7.4.1 Types of attacks detected	31
7.4.2 NIST PAD Evaluation	32
7.5 Detection of injection attacks	33
7.5.1 Security measures against injection attacks.....	33
8. Error handling in the identification process.....	34
8.1 Errors while scanning the document.....	34
8.2 Errors in the Selfie phase.....	35
8.3 Errors in the Video Phase	36

1. Introduction

IG PERSONA is the solution developed by Intesi Group to ensure the security and reliability of identification processes, in accordance with the requirements of ETSI TS 119 461, as required by EU Regulation 2024/1183 (eIDAS2) and Commission Implementing Regulation (EU) 2025/1566.

2. Overview

IG PERSONA is a comprehensive and flexible solution for orchestrating digital onboarding processes, designed to ensure maximum regulatory compliance, a high level of security, and a simple, guided user experience.

The platform allows you to manage multiple identification methods from a single integration point, reducing technical and operational complexity while ensuring a reliable identification process focused on data quality.

Based on a modular architecture, IG PERSONA is designed to integrate future developments in digital identity, such as the EUDI Wallet, and is on track for ETSI TS 119 461 v2.1.1 certification.

At the time of writing, the solution integrates the IG PERSONA Selfie and IG PERSONA Video identification methods.

3. Logical Architecture

The following is the logical diagram of the IG PERSONA solution, illustrating the integrations with external components and the flow of the identification process.

The diagram shows the **XpressID** component, integrated within the presentation layer of IG

PERSONA. The **VeriDas** technology component provides the identity verification service through communication with its proprietary cloud services.

XpressID, activated as soon as the QR Code is displayed, manages the entire document acquisition phase, up to the capture of the selfie and video for biometric verification.

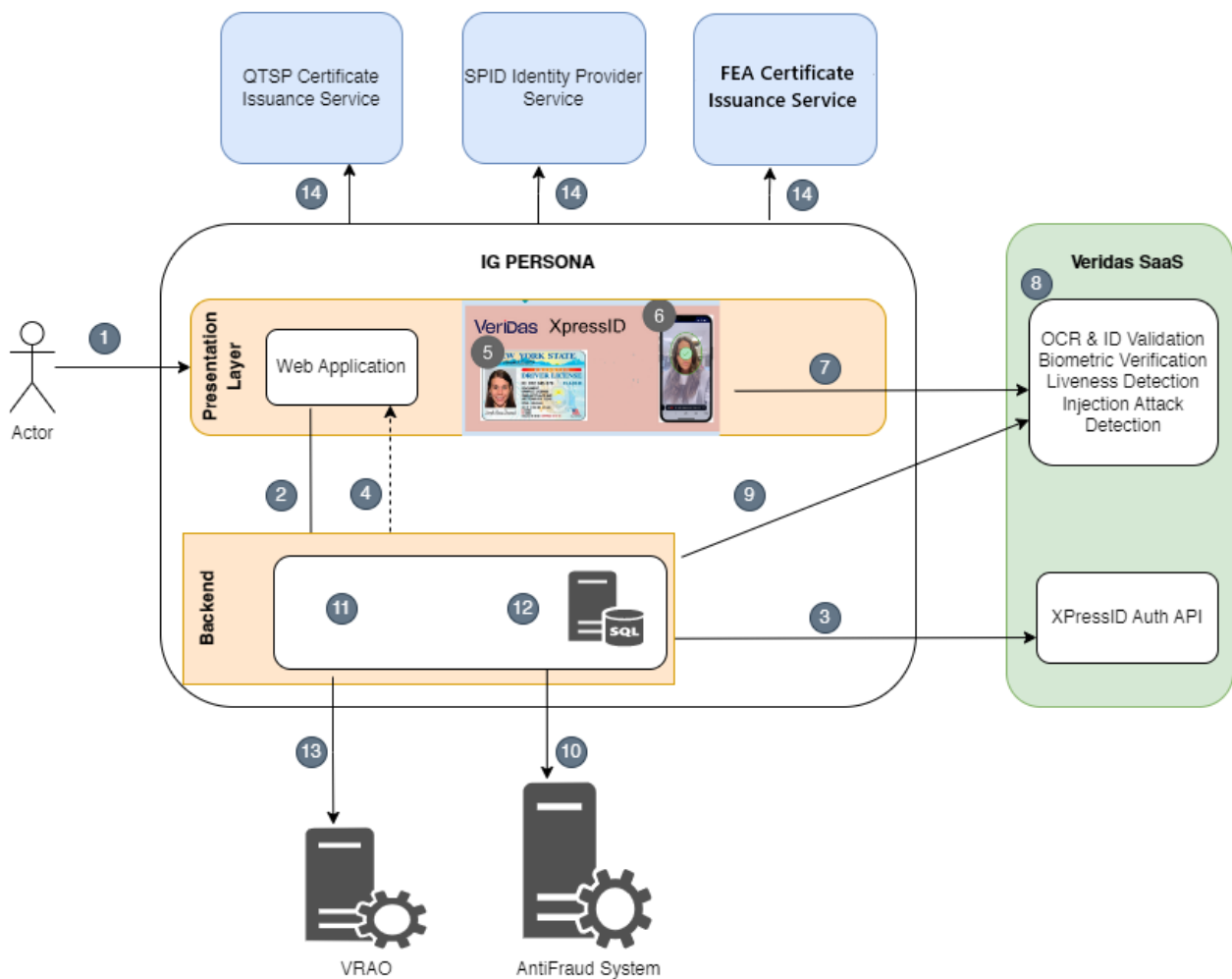


Figure 1. Logical architecture and workflow

IG PERSONA interacts with the following external systems:

- QTSP Certificate Issuance Service - Management of the qualified certificate issuance service.
- FEA Certificate Issuance Service - Management of the FEA certificate issuance service.
- SPID Identity Provider - Digital identity service (eID) notified within the Italian regulatory framework.
- VRAO - Archiving of evidence generated during the identification process.
- Anti-Fraud System - Anti-fraud system developed by Intesi Group and integrated into the identification workflow.

4. IG PERSONA Selfie/Video

IG PERSONA, in Selfie and Video modes, is the solution developed by Intesi Group that allows customers to complete the identification process independently.

The process can be carried out entirely on a smartphone or in hybrid mode, by starting the session on a desktop and completing the capture of evidence via smartphone, in a simple and intuitive manner.

The entire procedure is guided by text and visual instructions, which walk the user through the process step by step until completion.

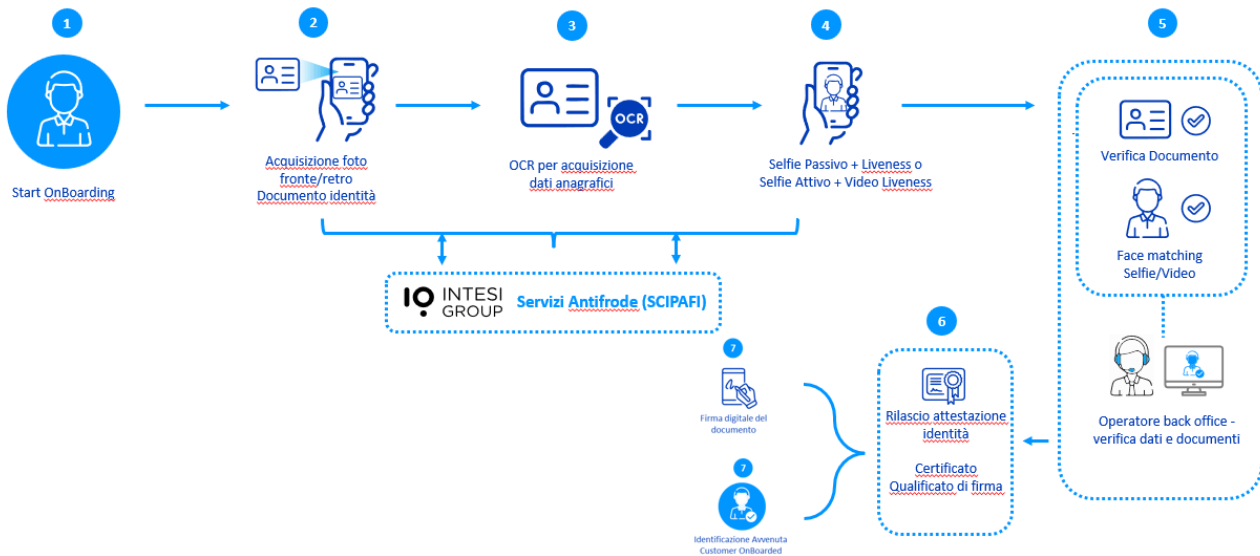


Figure 2. User Journey

4.1 Identification process

1. The user accesses the IG PERSONA web application to begin the onboarding process and accepts the terms and conditions of service.
2. The web application communicates with the backend service to request the initiation of the identity verification process.
3. The backend system requests a unique access token from the VeriDas Identity Verification Service (VeriDas CORE) to execute the onboarding flow.
4. The XpressID component is launched within the web application using the access token obtained.
5. The user captures the front and back of their ID card or passport.
6. The user performs the liveness check (active or passive), with the possible capture of a video.
7. The XpressID component sends the captured evidence to the VeriDas Identity Verification Service (VeriDas CORE) via a secure channel.

8. The VeriDas Identity Verification Service (VeriDas CORE) processes the acquired evidence:
 - a. Extraction of OCR data from the document and document validation (replay attack | print attack).
 - b. Biometric comparison between the photo printed on the document and the selfie.
 - c. Physical presence check (liveness).
 - d. Verification of injection attacks.
9. The backend system calls the VeriDas Identity Verification Service (VeriDas CORE) to obtain the outcome of the onboarding process, including OCR data, images, and validation scores.
10. The anti-fraud system performs a scoring assessment and interacts with any third-party services integrated into the solution, such as Scipafi.
11. An automatic decision is made to accept or reject the transaction.
12. The backend system stores the digital identity information.
13. The backend system archives the identification records in the VRAO NFS storage.
14. In the case of a synchronous in-person process, the validated process can proceed to the next steps.

4.2 Onboarding Process

The process begins when the customer accesses the IG PERSONA solution via a unique identification link.

The link can be obtained in one of the following ways:

- Via API - Application integration for programmatic initiation of the process.
- Via the Operator Portal - Manual initiation of the process for in-person identification (deVisu).
- Via email - Sending the link to the customer for remote execution.

Before starting the document capture, the customer is asked to confirm or enter their personal data: first name, last name, email address, and phone number (cell phone). The contact information is verified using a verification code, sent first via SMS and then via email.

After accepting the privacy policy and consenting to the processing of special categories of personal data, the customer may proceed with identity verification.

4.3 Scanning of identification documents

Depending on the type of document, the customer selects the method they wish to use for identification.

For Italian documents, the following are accepted:

- Electronic Identity Card (CIE)
- Driver's license
- Passport

For Italian documents, the process also requires the scanning of the Tax Code.

For non-Italian documents, the following are accepted:

- National identity document from the country of origin
- Passport

The procedure is guided by specific instructions that accompany the customer through every step of the process, ensuring a simple and intuitive experience.



Figure 3. Select document type

This phase is managed by the XpressID component, and the process is interrupted only if the type of document presented does not match the one selected by the customer. In such cases, a specific error message informs the user and prompts them to repeat the capture process, starting again with the selection of the document type.

No automatic assessments are performed on the quality of the scanned images.

Specific messages prompt the customer to verify the legibility of the document before proceeding, in order to ensure proper validation and reading of the data it contains.

4.4 Liveness check

The physical presence verification process can be performed in two ways:

- IG PERSONA Selfie (passive mode): the customer is asked to take a simple selfie for facial recognition.
- IG PERSONA Video (active mode): in addition to the selfie, the customer is asked to perform a double head movement following the instructions provided on the screen.

The active mode ensures a higher level of physical presence verification compared to the passive mode, as it requires dynamic interaction on the part of the customer during the capture.

In the active mode, if the movements made by the customer do not match those requested, a specific error message informs them of the discrepancy.

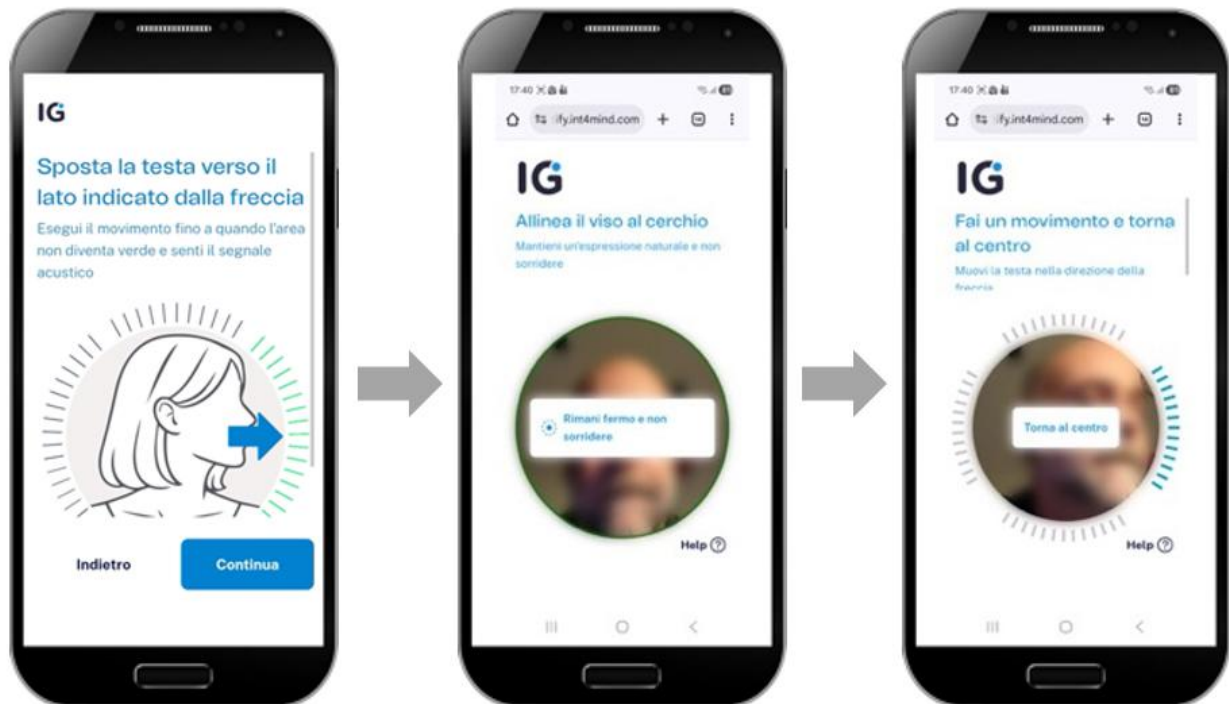


Figure 4. Active Selfie Motion Capture

4.5 Video with voice interaction

In the IG PERSONA Video mode only, the final step involves recording a short video in which the customer is asked to state their first and last name and to show the front of their identification document—that is, the side with their photo—to the camera.

The purpose of this step is to confirm intent: the customer does not take on a passive role, but

through both verbal and physical interaction reinforces the legal compliance of the entire identification procedure.

In this step, the workflow does not include interruptions or blocking error messages.

If the conditions for capturing the document are not optimal, specific messages guide the customer to adjust the framing or the environmental conditions, keeping the process on hold until the capture is complete.

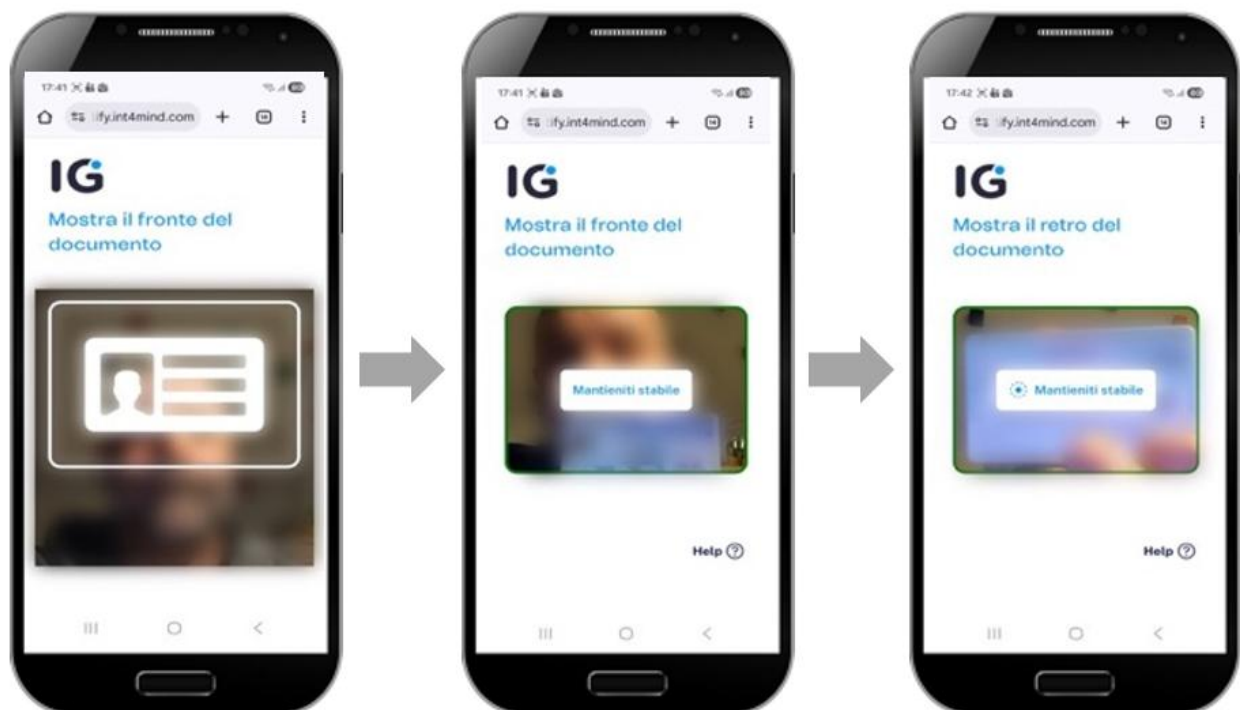


Figure 5. Video capture with document

4.6 Review and completion of the process

Once all steps of the identity verification process have been completed, the customer is directed to a summary page where they can review all the evidence and data collected during the procedure.

The following personal details are automatically pre-filled based on the information extracted from the document:

- First name
- Last name
- Date of birth
- Identification document details

The customer retains full control over their data: before proceeding with the final submission, they have the opportunity to verify the pre-filled information and make any necessary corrections.

Any changes made by the customer during the review phase will be subject to verification by the Anti-Fraud System, in order to detect and prevent fraudulent alterations to the acquired data.

4.7 National ID

The term “national identifier” refers to the national alphanumeric code that can be included in the qualified signature certificate. For Italy, the identifier is the tax identification number, while for other EU countries it may be the PNO (Personal Identification Number).

The national identifier, as shown below, is managed during the review phase and allows for the following scenarios:

- A customer with an Italian identification document who requests the inclusion of the tax code.
- A customer with a non-Italian identification document who requests the inclusion of the tax code.
- A customer with a non-Italian identification document who requests the inclusion of the 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. National ID on the review page

If a customer with an Italian identification document does not present their Health Card during the identity verification process, this section is marked as required, and in addition to entering their tax identification number, they must provide proof by manually uploading documents that verify the number, such as the tax identification number assignment certificate or the AIRE certificate that includes the number.

In the case of a customer with a NON-Italian identification document, they may be asked to enter the tax identification number within the qualified digital signature certificate by selecting the appropriate section and attaching the required document.

4.7.1 Identity verification without a health card (only for customers with an Italian ID)

In IG PERSONA Video mode, if a customer who holds an Italian identification document does not have a health insurance card, they can select the appropriate checkbox to proceed with identity verification.

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. Identity verification without a health insurance card

When this option is selected, the customer is shown a message informing them that they must supplement the tax ID entry by attaching additional documents to verify their national identification number.

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. Identity verification without a health insurance card

As described above, during the review phase, the customer must complete the process by entering their tax ID number and uploading the required document.

It will then be the back-office operator's responsibility to verify the submitted documentation in order to proceed with the approval of the identification process.

4.8 Backoffice operator

In applicable scenarios, the back-office operator intervenes to validate the data and evidence collected during the identification process.

In IG PERSONA Video mode, the identification process always requires validation by the operator.

In IG PERSONA Selfie mode, the operator intervenes based on the applicable scenario, as described in the following chapter.

The validation process is always performed via the RAO Portal (PkRA); as noted in the product release notes, a dedicated dashboard, complete with evidence and scores, allows the operator to make a more objective and accurate assessment.

5 Use Cases for IG PERSONA

The identification process via IG PERSONA enables a level of extended identification, a mandatory requirement for the provision of qualified services under the new eIDAS Regulation 2. With less restrictive criteria, the solution can also be adopted for those services for which a level of substantial identification is sufficient.

The process can be carried out using two identification methods:

- **In-Person Mode**

The process is initiated directly by the designated recognition officer (RAO), who guides and assists the customer during the procedure in person.

- **Remote Mode**

The customer, starting from the process initiation link, independently carries out the identification process; the operator intervenes subsequently to verify the evidence and data collected during the procedure.

Below is a summary of the scenarios supported by the IG PERSONA identification processes Selfie or Video:

Level (LoIP)	Service	IG PERSONA Scenario	Identification mode	Required evidence
Substantial	Advanced Signature	SELFIE	Remote	Front/Back Document + Selfie + Liveness Passive
Substantial	Advanced Signature	SELFIE AUTO_APPROVE	Remote	Front/Back Document + Selfie + Liveness Passive
Substantial	Advanced Signature	SELFIE AUTO_ENROLL	Remote	Front/Back Document + Selfie + Liveness Passive
Extended	Qualified Signature – Smart Card	SELFIE	In person	Front/Back Document + Selfie + Liveness Passive
Extended	Qualified Signature – Remota	SELFIE	In person	Front/Back Document + Selfie + Liveness Passive
Extended	SPID – Digital Identity	SELFIE	In person	Front/Back Document +

				Liveness Passive
Extended	Qualified Signature – Remote	VIDEO	Remote	Front/Back Document + Liveness Active + Video
Extended	SPID – Digital Identity	VIDEO	Remote	Front/Back Document + Liveness Active + Video
Extended	Qualified Seal	VIDEO	Remote	Front/Back Document + Liveness Active + Video

The documents accepted vary depending on the customer's nationality. For Italian citizens, a health insurance card is generally required for Extended-level processes.

5.1 LoIP Substantial – Advanced Signature

5.1.1 SELFIE - Remote mode

The customer receives an email containing a link to start the identification process via IG PERSONA SELFIE.

- Evidence collected - F/B Identification document + Selfie + Passive Liveness
- Back-office operator - Always required; verifies the collected evidence, views the scores, and approves or rejects the identification. In case of rejection, the customer receives a new email to repeat the identification process.
- Service Issuance - Upon approval by the back office operator, the customer receives an email to proceed with the issuance of the certificate.

- Supported Documents
 - Foreign: ID Card / Driver's License / Passport
 - Italy: CIE / Paper ID Card / Driver's License / Passport

5.1.2 SELFIE AUTO_APPROVE | Remote mode

The customer receives an email containing a link to start the identification process via IG PERSONA SELFIE.

- Data collected - F/B ID document + Selfie + Passive Liveness
- Back-office operator - The ANTI-FRAUD system synchronously verifies the collected data. If the verification is successful, the operator does not intervene, and the customer directly receives the email for certificate issuance. Otherwise, the back-office operator intervenes to validate the data.
- Service Provision - The customer receives an email to proceed with the issuance of the certificate.
- Supported Documents:
 - International: ID Card / Driver's License / Passport
 - Italy: CIE / Paper ID Card / Driver's License / Passport

5.1.3 SELFIE AUTO_ENROLL | Remote mode

The customer receives an email containing a link to start the identification process via IG PERSONA SELFIE.

- Data collected - F/B Identification document + Selfie + Passive Liveness Check
- Back-office operator - The ANTI-FRAUD system synchronously verifies the acquired data. If the verification is successful, the operator takes no action; and the customer directly receives the email confirming the issuance of a certificate. Otherwise, the back office operator intervenes to validate the data.

- Service Issuance - The customer receives an email confirming the issuance of the certificate.
- Supported Documents:
 - International: ID Card / Driver's License / Passport
 - Italy: CIE / Paper ID Card / Driver's License / Passport

This identification method supports only the issuance of certificates with OTP via SMS or email.

5.2 LoIP Extended

5.2.1 Qualified Signature – Smart Card | SELFIE | In person mode

The authorized RAO operator initiates and conducts the in-person verification via IG PERSONA SELFIE, in the physical presence of the customer.

- Data collected - Front/Back of ID document + Front/Back of Health Card (Italian citizens) + Passive Selfie
- Identity verification - The ANTI-FRAUD system synchronously verifies the acquired data (max 2 retries). If the verification is successful, the operator may proceed with approval. Otherwise, the process is suspended pending validation by the SUPERVISOR operator, who receives an email notification to approve or reject the identification. Once the SUPERVISOR has completed their assessment, the RAO operator is notified via email to resume the process and approve the identification.
- Service Issuance - Issuance of the certificate on a Smart Card, directly by the operator via IG DESK.
- Supported Documents:
 - Foreign: ID Card / Passport
 - Italy: CIE / Driver's License / Passport + Health Card

5.2.3 Qualified signature – Remote | VIDEO | Remote mode

The customer receives an email containing a link to start the identification process via IG PERSONA VIDEO.

- Evidence collected - Front/back of ID document + front/back of health card (Italian citizens) + active selfie + video
- Back-office operator - The operator verifies the collected evidence, reviews the scores, and approves or rejects the identification. In case of rejection, the customer receives a new email to repeat the process.
- Service issuance - The customer receives an email to proceed with the issuance of the qualified electronic signature certificate.
- Supported Documents:
 - Foreign: ID Card / Passport
 - Italy: CIE / Driver's License / Passport + Health Card

5.2.4 SPID – Digital Identity | VIDEO | Remote

The customer receives an email containing a link to start the identification process via IG PERSONA VIDEO.

- Evidence collected - Front-of-face photo of ID document + Front-of-face photo of health card + Active selfie + Video
- Back-office operator - The operator verifies the collected evidence, reviews the scores, and approves or rejects the identification. If rejected, the customer receives a new email to repeat the process.
- Service activation - The customer receives an email to proceed with the issuance of the SPID application.
- Supported documents:
 - Italy only: CIE / Driver's license / Passport + Health card

6. Score calculation and process validation

The calculation of the score used to validate each identification process is managed by the Antifraud System component, developed entirely by Intesi Group.

Through specific control procedures and warning thresholds, the system implements the following modalities:

- Antifraud Lite: a process for assessing data compliance and format, the uniqueness of contact information per user ID, and verification of whether the Italian tax ID is on a blacklist;
- Antifraud Scipafi: an anti-fraud assessment process via querying the Scipafi system— only for identification using Italian documents;
- Antifraud Veridas: evaluation of scores obtained at the end of the identity verification process. At the end of this phase, the identification process may be completed, interrupted, or proceed to the operator-assisted verification phase.
- Antifraud Complete: anti-fraud evaluation process that performs all required checks

The scoring process is enabled based on a specific profile that activates the various modes described above.

The system supports two types of workflows:

- Synchronous Workflow - The score calculation is performed immediately within the identification process, executing all enabled scoring processes.
- Asynchronous Workflow - The score calculation is deferred and managed via an event-based mechanism.

6.1 Antifraud Veridas

The process manages the scores generated and returned by the Veridas Digital Onboarding service upon completion of the identification document analysis and biometric evaluation.

Score-DocumentGlobal

Primary score for the identity document verification process. It verifies the authenticity and validity of the document presented.

The following scores are generated and returned by the Veridas Digital Onboarding service upon completion of the analysis of the selfie photo and video.

ValidasScoreSelfie

Main score for the similarity analysis between the selfie photo and the face photo on the identity document.

Indicates the probability that the two faces belong to the same person.

ValidasScoreVideo

Indicates the probability that the selfie photo and the face detected in the selfie video belong to the same person.

This score is evaluated only in the IG PERSONA Video identification mode.

ValidasScoreLifeProof

Indicates the probability that the person in the image is actually alive (liveness detection).

ValidasScorePhotoId

Indicates the probability that the selfie and the photo of the face on the ID document belong to the same person.

ValidasScoreSelfieAuthenticity

Indicates the probability that the selfie is authentic and not the result of a spoofing attempt.

The following score is generated and returned by the Veridas Digital Onboarding backend service for each captured image, upon completion of the integrity check. These scores ensure that the images captured via XPressID have reached the backend application without having undergone any modifications during transmission.

ValidasScoreIntegrity

Indicates whether the integrity of the entire validation process has been satisfied. The value depends on the following factors:

- The integrity score is available only if at least one of the images was
- captured using an SDK that supports the integrity feature.
- The value will be 1 if all uploaded images have an integrity score of 1.
- The value will be 0 if at least one of the images has an integrity score of 0

Based on these primary scores, the ValidationGlobalScore is calculated, representing the overall outcome of the entire validation process.

The main scores have a decimal (float) value between 0 and 1 and indicate, in a summary manner, whether a given process has concluded with a positive or negative outcome. Their use simplifies the evaluation of the result, sparing the customer from having to individually analyze an increasing number of detailed scores.

The main scores are as follows:

- Score-DocumentGlobal

- ValidasScoreSelfie
- ValidasScoreVideo
- ValidasScoreLifeProof
- ValidasScoreIntegrity

The values of these scores can be classified as follows:

- Valid - The value is high enough to be considered positive.
- Inconclusive - The evidence requires review by a human operator to determine its validity.
- Rejected - The value is low enough to be considered incorrect, potentially fraudulent, or otherwise unsuitable.

The following table lists the value ranges corresponding to each classification:

Main score	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

ValidasScoreIntegrity does not have an “Inconclusive” status: the value is always binary (1 = integrity confirmed, 0 = integrity not confirmed).

The ValidationGlobalScore takes one of the following three values, depending on the conditions listed:

Condition	ValidationGlobalScore value
All Score-DocumentGlobal, ValidasScoreSelfie, ValidasScoreLifeProof, ValidasScoreVideo, and ValidasScoreIntegrity scores are in the “Valid” status.	1

Only one of the scores listed above is marked as “Inconclusive.”	0.5
At least one of the scores listed above has a status of “Rejected,” or more than one has a status of “Inconclusive.”	0.0

7. Overview of VeriDas Technology

Let’s now take a closer look at the proprietary technologies developed by our technology partner VeriDas and integrated into the IG PERSONA solution.

7.1 ID Validation

Veridas’ OCR engine is developed entirely in-house and has been specifically trained to read all OCR fields on identity documents. Once the document has been scanned, the system returns all visible information from the scanned document, including both the front and back, ensuring over 99% accuracy in most fields.

The engine supports OCR reading in any language and in the following alphabets: Latin, Arabic, Chinese, and Cyrillic, including special characters.

The quality of validation depends on two main factors: the document’s intrinsic security level (documents with higher security measures offer more reliable digital verification) and the scanning technology used.

7.2 Document security checks

The system performs the following checks to verify the authenticity of the document presented:

1. Verification of expiration date and age of majority: the system verifies that the document has not expired and that the holder is of legal age.

2. Verification of MRZ checksums: the system reads and verifies the checksums of the MRZ (Machine Readable Zone) of the identity document.
3. Verification of consistency between visual data (VIZ) and MRZ: the system verifies the degree of correspondence between the data written in the document (VIZ) and the data reported in the MRZ.
4. Detection of black-and-white photocopies.
5. Detection of color photocopies: the system is capable of detecting the presence of color photocopies on various types of media (office paper, photo paper, laminated documents, polycarbonate, etc.).
6. Detection of documents displayed on screens: the system is capable of detecting the presence of various types of screens (smartphones, tablets, and desktop computers).
7. Detection of photo alteration or replacement on the document: the system identifies situations where a photo has been superimposed over the original photo on the document.
8. Detection of documents generated using artificial intelligence (deepfakes) and digital manipulation: the system is capable of detecting total or partial image manipulation performed with programs such as Photoshop, as well as artificially generated documents.
9. Decoding of two-dimensional barcodes (OBR): The system supports various formats (Code 128, Code 39, Barcode, DataMatrix, QR, and PDF417) and compares the data printed on the document (VIZ and MRZ) with the data encoded in the two-dimensional barcodes to verify consistency.

7.3 Biometric verification

Veridas offers cutting-edge facial biometric technology based on artificial intelligence systems trained with deep neural networks for facial recognition. The biometric engine is developed

entirely in-house and undergoes continuous evaluation by the NIST (National Institute of Standards and Technology), regularly achieving top rankings in international assessments. The engine enables comparisons between two images (selfies or faces on official identity documents) to determine whether they belong to the same person. The system analyzes the facial image and converts it into an irreversible mathematical vector, making it impossible to recover the original image if that vector is deleted, thereby ensuring the protection of the user's privacy at every stage of the process.

7.3.1 NIST-certified accuracy

NIST is the U.S. federal agency that serves as the international benchmark for the evaluation and classification of biometric engines. According to the report published by NIST for FRTE 1:N in April 2023, Veridas achieved a false negative rate (FNIR) of 0.0232 in the Mugshot category, with a false positive rate (FPIR) of 0.001, on a database of 12 million identities.

7.3.2 Absence of bias

Veridas' biometric engine does not exhibit any bias based on ethnicity, gender, or any other factor. Veridas is actively involved in the scientific community regarding biometric bias and has collaborated with the Universidad Autónoma de Madrid to define a new metric for measuring bias in biometric systems.

Biometric systems offer greater accuracy than facial recognition performed by humans. Studies from 2014 have shown that people achieve 97.53% accuracy in facial recognition, while algorithms exceed 99%. Unlike human biases - which cannot be objectively measured or audited - biases in biometric systems are objectively measurable and verifiable.

7.3.3 Biometric verification during the onboarding process

The Veridas biometric engine is capable of comparing a selfie with a photo cropped from an identity document, in accordance with ICAO standards. The engine has been specifically trained for this use case, optimizing performance under the following variable conditions:

- Presence of reflections in the area of the photo printed on the document.
- Presence of holograms (kinegrams) and other visual artifacts on the printed photo.
- Time difference between the selfie photo taken by the user and the photo on the document.
- Variations in facial appearance: presence of a beard, mustache, changes in hairstyle, glasses, makeup, etc.

The biometric comparison process is completed in less than a second. The engine returns a facial similarity score with a value between 0 and 1: the higher the value, the greater the probability that the two images belong to the same person. The customer can independently choose the decision threshold and modify it at any time based on the level of security required by their use case.

7.4 Liveness detection

Veridas offers proprietary liveness detection technology for detecting presentation attacks and deepfakes. The solution is certified by iBeta to ISO 30.107 at Levels 1 and 2, for both active and passive modes, in native and web environments.

Level 2 certification represents the highest standard available and is focused on detecting the most sophisticated attacks, passing tests conducted with realistic mannequins and 3D masks made of resin, latex, and silicone, as well as faces synthesized from digital images.

7.4.1 Types of attacks detected

The system is capable of detecting the following types of attacks:

- Screen-based attacks: the use of a screen to display an image of another person's face in front of the camera on the attacker's device.
- Video-based screen attacks: video playback showing the face of the person to be impersonated, which requires the full cooperation of the subject being imitated.
- 3D animation attacks: attacks in which the person's face is artificially generated and animated using software.
- Photographic print attacks: use of one or more prints of a human face in different print qualities.
- Printed mask attacks: printing the face on paper and cutting it out to construct a 2D mask.
- 3D photographic masks: composition of multiple printed photographs layered to simulate a three-dimensional effect.
- Latex masks: attack carried out by wearing a latex mask in front of the camera.
- Attacks using mannequins: attack carried out by placing a mannequin in front of the camera.
- Plaster masks: attack performed while wearing masks made of plaster and painted in detail.
- Rigid plastic masks: attack performed with a rigid plastic mask in front of the camera.
- Silicone masks: attack performed with a silicone mask in front of the camera.
- Transparent masks: attack performed using a translucent mask.

7.4.2 NIST PAD Evaluation

Veridas submitted its engine to the NIST PAD evaluation, which measures the ability to detect attempts to spoof images or videos, regardless of whether capture SDKs are used, ensuring consistent evaluation conditions for all manufacturers.

7.5 Detection of injection attacks

Identity fraud can be carried out in two different ways:

- **Presentation attack** - The attacker presents false evidence to the camera of the capture device, such as a photocopy, a screenshot, or any other attempt at impersonation.
- **Injection attack** - The attacker injects false evidence directly into the system without having to present anything to the camera, by manipulating the capture channel or the communication channel.

7.5.1 Security measures against injection attacks

The Veridas system implements the following security measures to detect injection attacks:

API Security - Veridas employs numerous security mechanisms that prevent the uncontrolled invocation of APIs for the injection of unauthorized content. These measures include the use of API keys, IP filters, and additional controls described in the Infrastructure and Security section.

Detection of Virtual Cameras - The system is capable of detecting instances where an attacker uses a virtual camera (e.g., VirtualCam) to inject an image of a document or a face into the system as if it had been captured by the device's actual camera.

Detection of emulators and other untrusted elements - Veridas has technology to verify the trustworthiness of the device from which the identity verification process is executed. The system is capable of detecting processes executed by emulated devices, virtual machines, bots, or active development environments, which are considered untrusted for performing the verification.

Detection via Business Intelligence Techniques - Veridas analyzes dozens of parameters related to the process to verify that it was executed completely, end-to-end from the same device, and without the use of evidence injected directly into the system.

The security measures described are logical in nature and not statistical: their detection

8. Error handling in the identification process

The following are possible error scenarios handled with appropriate messages during the identification process.

None of these scenarios prevent the customer from completing the identification process. The system handles errors by having the customer resubmit the step or by prompting them to restart the process from the start link.

8.1 Errors while scanning the document

Error type	Message title	Message for the customer
Camera activation failed.	The verification process could not be completed. Please try again.	The verification process could not be completed. Please try again.
Camera not detected	No camera detected.	To continue, please verify that your device has a camera.
Camera/Microphone Permissions	Permissions required.	Please make sure to allow the page access to your camera and microphone.
Incorrect device orientation.	Rotate your device.	To continue, hold your phone in portrait orientation.
Change in orientation during the process	Try the process again.	The process was not completed due to an unexpected change in the orientation of the device.
Document verification failed	Verification failed.	We were unable to complete the document verification process. Please try again and make sure the document meets the requirements.

8.2 Errors in the Selfie phase

Error type	Message title	Message for the customer
Camera activation failed.	Unable to activate the camera.	Something prevented the camera from starting up properly. Check to see if it is being used by another app, and try again.
Camera not detected	No camera detected.	To continue, please verify that your device has a camera.
Loss of focus	The process has been interrupted.	For security reasons, the verification was interrupted after detecting a switch to another application or tab. Restart the process to continue.
No movement detected	No head movement detected.	When prompted on the screen, move your head to the corresponding side and return to the center when the signal is given or when you hear the sound.
Camera/Microphone Permissions	Permissions required.	We cannot access your camera or microphone. Please enable permissions in your device settings or browser settings to continue.
Incorrect device orientation.	Rotate your device.	To continue, hold your phone in portrait orientation.
Change in orientation during the process	Retry the process.	The process was not completed due to an

		unexpected change in the orientation of the device.
Gesture verification failed	Verification failed.	It appears you made a different gesture than the one indicated. To continue, follow the arrow with your head at a moderate speed and return to the center when prompted.

8.3 Errors in the Video Phase

Error type	Message title	Message for the customer
Camera activation failed.	Unable to activate the camera.	Something prevented the camera from starting up properly. Check to see if it is being used by another app, and try again.
Camera not detected	No camera detected.	To continue, please verify that your device has a camera.
Camera/Microphone Permissions	Permissions required.	We cannot access your camera or microphone. Please enable permissions in your device settings or browser settings to continue.
Incorrect device orientation.	Rotate your device.	To continue, hold your phone in portrait orientation.
Change in orientation during the process	Retry the process.	The process was not completed due to an unexpected change in the orientation of the device.

