IDENTITY VERIFICATION SERVICE

Product Specification

Version	Date
[0.1]	[10/12/2024]

1 Introduction

Identity Verification Service (IVS) is a remote identity verification solution designed to streamline and secure the process of verifying a user's identity online. By combining advanced document scanning, facial biometrics, OCR (Optical Character Recognition), automated image capture, and robust liveness and spoof detection mechanisms, our solution ensures that you can confidently authenticate users in remote channels without compromising on user experience or security.

2 Key Features Overview

ID Document Scanning

- **Supported Document Types:**
  Our solution supports a wide range of government-issued IDs, including passports, driver's licenses, and national ID cards. The list of supported documents can be found here:
  https://developers.innovatrics.com/digital-onboarding/docs/functionalities/document/supported-documents/

- **High-Quality Image Capture:**
  The system guides users to position their ID documents correctly, automatically capturing clear, distortion-free images. This maximizes the accuracy of the subsequent recognition and verification steps.

- **Compatibility:**
  Works seamlessly across desktop and mobile devices, leveraging built-in or external cameras.

Optical Character Recognition (OCR)

- **Automated Data Extraction:**
  The OCR component extracts readable text from the captured ID image, including fields such as name, date of birth, document number, and expiration date.

- **Accuracy and Speed:**
  Our OCR engine employs machine learning algorithms to efficiently identify and convert text, ensuring low error rates and rapid processing.

- **Data Validation and Formatting:**
  Extracted data can be validated against known formats, reference databases, and business rules, ensuring only accurate and standardized information is passed forward.

Face Biometrics

- **Facial Recognition Engine:**
  The face biometrics module matches the selfie image captured by the user against the photo on their submitted ID. This includes comparing facial features, contours, and key points to ensure a high-quality match.

- **Robust Matching Algorithms:**
  Advanced neural network models improve accuracy even under challenging conditions (varying lighting, camera quality, or user posture).

Selfie Capture with Auto-Capture

- **Guided Capture Process:**
  The system guides the user on how to position themselves for optimal image

quality—centering their face, ensuring proper lighting, and removing any obstructions like sunglasses.

- **Automatic Snapshot:**
  Once ideal conditions are detected (proper focus, face alignment, and exposure), the system automatically takes the selfie. This reduces user friction and helps ensure consistent, high-quality images.

- **User-Friendly UX:**
  Simple on-screen prompts and a clean interface enhance user experience, reducing failed attempts and support queries.

Passive Liveness Check

- **Non-Intrusive User Experience:**
  Our passive liveness solution analyzes subtle facial movements, texture patterns, and other biometric signals to differentiate real, live individuals from still images or synthetic media—without requiring the user to perform any special actions like blinking or nodding.

- **Security Against Spoofing:**
  The liveness algorithm resists various spoof attempts, including printed photos, screen replay attacks, and simple face masks.

Video Injection Detection

- **Detection of Advanced Spoof Attacks:**
  This feature monitors the camera feed to identify whether the input is coming from a live camera source or a pre-recorded, manipulated video feed.

- **Real-Time Analysis:**
  By examining metadata, motion patterns, frame integrity, and other advanced signals, our system can quickly halt the verification process if video injection is detected.

- **Enhanced Security Layer:**
  Combined with passive liveness, video injection detection further ensures that only genuine, live individuals are verified, effectively countering more sophisticated fraud attempts.

3 Verification Workflow

01 **User Initiation**
The user starts the verification process by accessing the verification service via a web or mobile interface.

02 **ID Capture**
The user is prompted to hold their ID in front of the camera. The system automatically captures the best possible image once optimal conditions are detected.

03 **OCR Processing**
The captured ID image is processed by the OCR engine to extract and validate personal information.

04 **Selfie Capture**
The user is instructed to face the camera. Once alignment and focus are optimal, a selfie is automatically captured.

05 **Face Matching & Liveness Checks**
The selfie is matched against the ID photo. In parallel, passive liveness and video injection checks confirm that the user is physically present and not using any spoofing techniques.

06 **Result and Reporting**
The system consolidates all verification results—ID validity, extracted data accuracy, face match score, and liveness outcomes—and returns a final decision to the requesting system.

4 Trust Factors

Trust factors are key metrics or indicators used to assess the authenticity, integrity, and reliability of the identity verification process. They serve as data points that influence the overall decision on whether the presented identity is genuine. Trust factors can be represented as scores (numeric values) or Boolean flags (true/false outcomes).

In a table below are displayed trust factors with type and default values :

Trust factor	Type	Reject condition
Document face match	Score	<0.325
Document portrait not replicated	Score	>0.9
Passive liveness	Score	<0.8
Video injection detection	Boolean	TRUE
Document not expired	Boolean	FALSE
Document liveness	Score	<0.01
Document portrait substitution	Score	<0.5

In an identity verification system, these trust factors are typically combined and weighted according to business rules.

If any of these factors fail to meet set thresholds, the system may deny the verification. Trust factor thresholds (e.g., what score is considered a “pass”) are often configurable to align with varying security requirements, regulations, and user experience goals.