Scope Document for Liveliness & Face matching Service

Table of Contents

[1. Objective 2](#_Toc206671311)

[2. Key Deliverables 2](#_Toc206671312)

[3. Deployment & Data Sovereignty 3](#_Toc206671313)

[3.1. Strict On-Premises Deployment Mandate 3](#_Toc206671314)

[3.2. Complete Data Isolation and Local Storage 3](#_Toc206671315)

[4. Performance, Accuracy, and Algorithmic Requirements 4](#_Toc206671316)

[4.1. Human and Liveliness Detection (Presentation Attack Detection) 4](#_Toc206671317)

[4.2. Face Comparison (1:1 Biometric Verification) 5](#_Toc206671318)

[5. Customization & User Experience 5](#_Toc206671319)

[6. Session Management 5](#_Toc206671320)

[7. Customer Interface 5](#_Toc206671321)

[8. Security & Biometric Authentication Process 6](#_Toc206671322)

[9. Session Recording & Reporting 6](#_Toc206671323)

[10. Support & SLA Compliance 6](#_Toc206671324)

[11. Platform Support 7](#_Toc206671325)

[12. Integration Capabilities 7](#_Toc206671326)

[13. Security & Data Privacy 7](#_Toc206671327)

[14. Audit & Compliance Logging 7](#_Toc206671328)

[15. Feedback Mechanism 8](#_Toc206671329)

[16. Scalability Requirements 8](#_Toc206671330)

[17. Comply with Bank Information Security Policies 8](#_Toc206671331)

## 1. Objective

The primary objective of this Scope of Work (SOW) is to procure a specialized, enterprise-grade platform to establish a high-assurance binding between a digital identity and a physically present, live human being. The central and non-negotiable tenet of this procurement is that the solution must be deployed, operated, and managed entirely within the bank's own secure data centers.

The platform's purpose is to serve as the definitive gatekeeper for digital identity assertion, using a sophisticated, two-stage biometric process:

1. **Presence Assurance via Liveliness Detection:** First, the system must confirm with an extremely high degree of confidence that the individual presenting themselves for verification is a real, live person. This involves actively detecting and mitigating sophisticated fraud attempts known as Presentation Attacks.
2. **Identity Verification via Face Comparison:** Second, upon successful confirmation of liveness, the system must biometrically match the live facial image of the user to a trusted reference image, thereby verifying their claimed identity with quantifiable accuracy.

This solution will serve as a foundational security control, replacing manual, subjective visual comparisons with an automated, objective, and forensically auditable biometric verification process.

## 2. Key Deliverables

The vendor shall provide a complete, self-contained software solution that can be deployed on the bank's infrastructure. The solution must comprise the following key deliverables:

* **A Core Biometric Verification Engine:** This is the heart of the solution and must be delivered as a deployable software package (e.g., containerized application, virtual appliance, or installable binaries) for the bank's designated servers. This engine is not monolithic but a suite of interconnected microservices, primarily comprising:
  + **A Presentation Attack Detection (Liveness) Module:** This module contains the AI/ML models responsible for analyzing the video stream to detect signs of life and distinguish a real person from a fraudulent artifact.
  + **A Face Comparison (1:1 Verification) Module:** This module contains the advanced facial recognition algorithms for creating biometric templates and calculating the similarity score between the live selfie and a reference image.
* **Client-Side Software Development Kits (SDKs):** The vendor must provide secure, lightweight, and high-performance SDKs for all required client platforms. These SDKs are responsible for managing the user interaction, capturing the video stream, providing real-time feedback, and securely transmitting the data exclusively to the bank's on-premises instance of the Biometric Verification Engine.
* **A Secure Administrative Portal:** A self-hosted web application that provides a comprehensive interface for authorized bank personnel. It must be deployed within the bank's network and connect to the on-premises engine and database. Its functions must include, at a minimum: policy configuration (e.g., setting liveness thresholds), review queues for failed or low-confidence verifications, detailed session investigation tools, and access to performance analytics related to liveness and face comparison accuracy.
* **A Comprehensive Suite of Server-Side APIs:** A set of well-documented, versioned, and secure RESTful APIs exposed by the on-premises engine. These APIs are the primary method for the bank's other internal applications to initiate verification sessions and retrieve the detailed results of the liveness and face comparison checks.

## 3. Deployment & Data Sovereignty

This section outlines the most critical requirements of the solution, which are foundational to its acceptance. Deployment should include all necessary environments such as UAT, Pre-production, Production, and Disaster Recovery (DR)

## 3.1. Strict On-Premises Deployment Mandate

The proposed solution **must be an on-premises solution.** No cloud-based, hybrid-cloud, or vendor-hosted solutions of any kind will be considered. The vendor is required to provide the complete software package, including all necessary components, engines, databases, and dependencies, for installation and operation within the bank's own secure data centers and under the bank's exclusive control.

## 3.2. Complete Data Isolation and Local Storage

It is a paramount and non-negotiable requirement that **no information of any kind goes outside the bank's on-premises environment.** This principle of complete data isolation must be architecturally enforced.

* **Local Data Storage:** All data captured, generated, or processed by the system **must be saved and stored exclusively on the bank's on-premises servers.** This explicitly includes, but is not limited to, every **video** file from the liveness check, every captured **image** (selfie, reference photo), all generated biometric templates, and all system and audit **logs**.
* **No External Communication:** The deployed solution must operate in a completely self-contained manner. It is strictly forbidden for the software to make any outbound network calls to vendor-hosted or third-party cloud services for any purpose, including biometric processing, license key validation, system health checks, or the transmission of telemetry or analytics.

## 4. Performance, Accuracy, and Algorithmic Requirements

The utility of the solution is directly tied to its performance and accuracy. The vendor must provide verifiable, independent test results to substantiate their claims in these areas.

## 4.1. Human and Liveliness Detection (Presentation Attack Detection)

The solution's capability to correctly identify a live human being and reject fraudulent attempts **must be exceptionally accurate.**

* **4.1.1. Liveness Modalities:** The solution must support multiple liveness modalities to provide a flexible and robust defense. The vendor must describe their capabilities for both:
  + **Active Liveness:** A challenge-response mechanism where the user is prompted to perform a simple, randomized action (e.g., turning their head, smiling, blinking). This proves the user is live and can react to instructions.
  + **Passive Liveness:** A frictionless method that analyzes the video stream in the background for subtle, involuntary indicators of life without requiring specific user actions. This may include light reflection patterns, 3D depth perception, and natural micro-movements.
* **4.1.2. Spoofing Vector Resistance:** The platform must be specifically designed and tested to defeat a comprehensive range of presentation attacks. The vendor must provide details on the system's resilience against:
  + Printed Photos (high and low resolution)
  + Digital Screen Replays (photos and videos displayed on phones, tablets, and monitors)
  + 2D and 3D Masks (paper, silicone, resin)
  + Emerging threats such as Deepfakes and other forms of synthetic video.

## 4.2. Face Comparison (1:1 Biometric Verification)

The biometric face comparison algorithm **must demonstrate a degree of accuracy suitable for high-stakes financial transactions.**

* **4.2.1. Core Algorithm Requirements:** The vendor must provide performance statistics, including:
  + **False Acceptance Rate (FAR):** This measures the probability of incorrectly matching an individual to another person's identity.
  + **False Rejection Rate (FRR):** This measures the probability of failing to match an individual to their own valid identity. The vendor must provide the FRR at the specified FAR.  
    The algorithm must be robust against variations in lighting, pose, facial expression, accessories (e.g., glasses), and the effects of aging.
* **4.2.2. Bias and Fairness:** To ensure an equitable and inclusive process, the vendor must provide data demonstrating the algorithm's performance equity across different demographic groups (e.g., age, gender, ethnicity). The variance in FRR between demographic cohorts should be minimal to prevent any single group from experiencing a disproportionately poor user experience.

## 5. Customization & User Experience

The solution must deliver superior user experience. The client-side SDKs must be fully white-labelable, allowing the bank to control all aspects of the UI. The on-premises administrative portal must allow the bank to configure verification policies, such as the type of liveness check to perform and the specific confidence thresholds for both liveness and face comparison results.

## 6. Session Management

The platform must enforce robust session management for every biometric transaction, utilizing secure, short-lived tokens generated and validated by the bank's on-premises servers.

## 7. Customer Interface

The user interface for the biometric capture process must be meticulously designed for clarity and a high first-time success rate. It must provide real-time, interactive feedback to guide the user in correctly positioning their face, ensuring optimal lighting, and successfully completing any required liveness actions.

## 8. Security & Biometric Authentication Process

The platform's security model relies on a strict, sequential biometric authentication process:

1. **Stage 1: Liveness Verification (The Gatekeeper):** The first and most critical step is the liveness check. The system analyzes the user's video stream to confirm genuine human presence. A face comparison is **never** attempted if the liveness check fails. This prevents fraudulent artifacts from ever being processed by the facial recognition algorithm and ensures that system resources are not wasted on obvious spoofing attempts.
2. **Stage 2: Face Comparison (The Confirmation):** Only after a user has successfully passed the liveness verification will the system proceed to the face comparison stage. The system will then create a biometric template from the verified-live selfie and compare it against the template from the trusted reference image.

This two-stage process ensures that the identity verification is both secure and efficient, providing a high-assurance result.

## 9. Session Recording & Reporting

The platform must securely record and store all artifacts from each verification session **directly onto the bank's on-premises storage infrastructure.** This includes the full video of the liveness check, high-resolution selfie images, and detailed logs. The administrative portal's reporting engine must operate exclusively on this locally stored data, providing detailed analytics on:

* **Liveness Performance:** Success/failure rates, breakdown of failures by type (e.g., poor lighting, detected spoof attack), and types of attacks detected.
* **Face Comparison Performance:** Distribution of confidence scores, match/no-match rates, and analysis of false rejection trends.

## 10. Support & SLA Compliance

The vendor must provide enterprise-level technical support, and an SLA tailored on-premises software, covering support response times, bug-fix timelines, and guaranteed availability of security patches and version updates. SLA should include the following terms also-

* Provision of a ticketing system for issue tracking and resolution management.
* 24/7 vendor technical support with SLA-backed response timelines based on severity.

## 11. Platform Support

The solution’s client-side SDKs must function flawlessly and be fully supported across the latest two major versions of all major web browsers and recent versions of mobile operating systems.

## 12. Integration Capabilities

The solution must be designed for secure integration within the bank's ecosystem. All API endpoints will be hosted on the on-premises servers. The platform must also support webhook notifications to other internal bank systems, providing detailed results of the liveness and face comparison checks.

## 13. Security & Data Privacy

With the on-premises mandate, the bank retains full control over its data. The solution must support this with features like end-to-end encryption for data in transit within the bank's network and a granular Role-Based Access Control (RBAC) model for the administrative portal.

## 14. Audit & Compliance Logging

The platform must generate a definitive, immutable log for every biometric transaction. These logs **must be written to and stored on the bank's on-premises logging servers** and contain specific, detailed fields for forensic analysis, including:

* liveness\_result: pass/fail
* liveness\_score: [quantifiable score]
* detected\_attack\_type: [e.g., screen\_replay, printed\_photo, none]
* face\_match\_result: pass/fail
* face\_match\_score: [e.g., 0.9987]

• Maintain detailed, timestamped logs capturing session start/end, user actions, and elements accessed or interacted with.

• Track detailed user activity timelines during sessions.

• Log API requests and responses, including exception messages to facilitate troubleshooting and root cause analysis.

## 15. Feedback Mechanism

The solution should optionally offer a method to gather user feedback regarding their experience with the biometric verification step. This feature must be configurable and, if enabled, all collected feedback data must be stored exclusively within the on-premises environment.

## 16. Scalability Requirements

The vendor must provide detailed hardware and infrastructure requirements. The architecture must support both vertical and horizontal scalability within the bank's data center to ensure high availability and performance under heavy load.

## 17. Comply with Bank Information Security Policies

The proposed on-premises solution must fully comply with all of the bank's Information Security policies. The vendor must provide detailed installation, configuration, and security hardening guides and agree to cooperate fully with the bank's security teams during all phases of the project.

**Vendor has to submit a Company Profile along with the Technical & Commercial Documents.**