Shufti

Biometric Face Authentication

Authenticate the right person, every time.

Verify the real user behind every interaction with biometric authentication.

The Challenge with Traditional Authentication

Credentials are not identity.

Organisations invest significantly in verifying identity at onboarding, but the point of entry is only the beginning. As fraud grows more sophisticated and regulatory expectations rise, continuously confirming identity throughout the customer lifecycle has become a business-critical requirement.

Yet the methods most organisations rely on share a common limitation: they authenticate credentials, not people. Knowing a password, receiving a code, or possessing a device provides no assurance that the person behind the interaction is the same person who opened the account.

This is precisely where fraud takes hold, and the consequences of overlooking it are significant.

Passwords

Exposed through credential stuffing, brute force, and phishing attacks, while creating friction that undermines the customer experience.

One-Time Passcodes (OTPs)

Vulnerable to SIM-swap fraud and code interception, with the added burden of friction at every authentication event.

Authenticator Apps

Complex to configure and poorly adopted, particularly among non-technical users, limiting their effectiveness at scale.

The cumulative effect is an authentication landscape that leaves organisations exposed to account takeover, payment fraud, and compliance risk, while placing unnecessary burden on legitimate customers.

What is Biometric Face Authentication ?

Biometric Face Authentication is a method that confirms a person's identity by comparing a live capture, typically a selfie or liveness check against a single, specific stored biometric profile: the one created for that individual at enrollment.

Introducing Shufti Biometric Face Authentication

Shufti Biometric Face Authentication is a continuous biometric identity verification solution designed for both enrollment and ongoing authentication. Rather than relying on credentials a user knows (passwords) or possesses (OTPs), Shufti Biometric Face Authentication verifies identity based on who the user actually is by matching a live biometric capture against the unique facial identifier established at onboarding.

Shufti Biometric Face Authentication is designed for the most critical and recurring moments in a user's lifecycle

Enrollment

Secure capture of the biometric profile at account creation, establishing the identity anchor used in all future authentication events.

Login Authentication

Continuous identity assurance at every session, replacing passwords and OTPs with a biometric liveness check.

Step-Up Authentication

Triggered for high-risk actions such as changing account details or adding a beneficiary, applying a stronger layer of verification without adding friction.

Action-Based Authentication

Biometric confirmation at the point of a specific event, such as making a payment, executing a withdrawal, or reaching a transaction threshold.

Account Recovery

Identity-assured recovery replacing knowledge-based questions and vulnerable reset links.

Bulk Migration Enrollment

Onboard existing user bases via CSV when migrating from a legacy platform, with no individual re-registration required.

How Shufti Biometric Face Authentication Works?

Step 1

User Enrollment

The Biometric Face Authentication process begins with a user securely enrolling their facial data. During this stage:

- The user captures a selfie or facial image using a trusted device.
- The system performs quality checks to ensure the image meets required standards (lighting, clarity, face position, and liveness).
- Advanced facial recognition algorithms extract biometric features from the image and convert them into a secure facial template and associate them against a unique customer identifier.
- The facial template and the unique identifier are securely stored together as a reference record.

Step 2

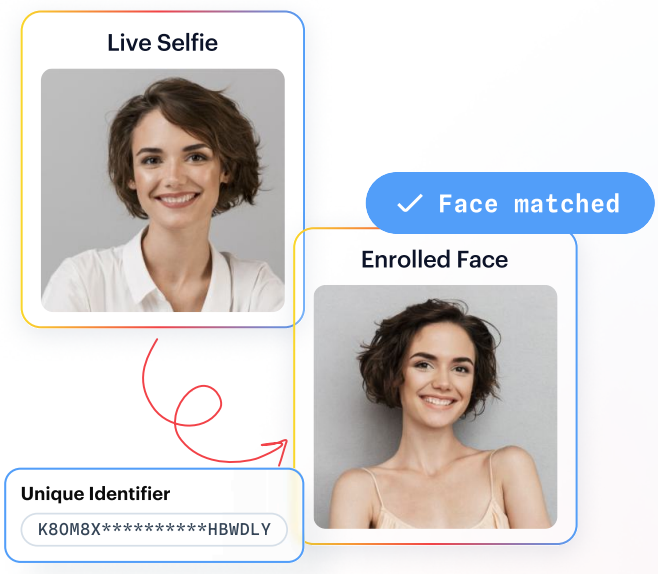
User Authentication

When the user later attempts to authenticate:

- The request is initiated by passing the customer identifier of the user.
- The end user journey begins with a live facial image capture.
- Liveness detection mechanisms are applied to ensure the presence of a real person and prevent spoofing attempts using photos, videos, or masks.
- The live facial template is matched directly against the enrolled facial template.
- If the Liveness checks is passed and the facial image matches with the stored template the user is authenticated successfully.

Why Shufti Biometric Face Authentication?

Shufti Biometric Face Authentication closes the gap that legacy methods leave open, the inability to confirm that the person behind the interaction is the same person who opened the account. Every authentication event is anchored to the verified biometric identity established at onboarding, delivering continuous identity assurance across every critical moment in the customer lifecycle.



Feature	What It Means for You
High Accuracy	Direct matching against a single reference reduces false positives and false negatives.
Faster Performance	No database-wide searches, enabling near-instant verification.
User-Friendly Experience	Simple selfie-based authentication without passwords or physical documents.
Continuous Identity Assurance	Authentication event is matched 1:1 against the unique biometric identity established at onboarding, ensuring the right person is confirmed at every critical action, not just at the point of entry.
Deepfake & Injection Detection	Identifies face swaps, morphed images, virtual cameras, and emulator-based injection attacks before a match is attempted, ensuring the integrity of every authentication event.
Regulatory Alignment	Step-up authentication designed to meet key regulations such as PSD2 Strong Customer Authentication (SCA) requirements, reducing compliance risk across regulated markets.
Owned Technology Stack	Built entirely on proprietary biometric infrastructure with no third-party dependencies, giving full control over accuracy, performance, and the security of every authentication event.
World-Class Benchmark Performance	Shufti's face verification was independently validated in the 2025 DHS RIVR benchmarks where Shufti met 100% of DHS goals for biometric accuracy across diverse demographics.
Flexible Deployment	Cloud: Fully managed: Shufti infrastructure; On-Premises: Full data sovereignty: your environment and Hybrid: Split model: privacy + performance
Onsite verification	Shufti directly interact with the end user, managing data collection to facilitate Biometric Face Authentication. Verification status updates are communicated to the client via callback URL and the Shufti back office.
Offsite verification	Client is responsible for collecting the required proofs and information from the end user and submitting it to Shufti for verification.

Industry Use Cases

Shufti Biometric Face Authentication is **purpose-built for sectors** where the cost of identity failure is high and the expectation of a seamless user experience is non-negotiable.

Fintech

Biometric authentication at login, payment confirmation, and account changes ensures that sensitive financial actions are always performed by the verified account holder, supporting SCA compliance and reducing exposure to account takeover fraud.

Crypto

Continuous identity assurance at wallet access, withdrawal execution, and transaction threshold events protects against unauthorised asset transfers in an environment where transactions are irreversible.

Forex

Step-up authentication for high-value trades, fund withdrawals, and leverage adjustments ensures that critical trading actions are tied to a verified identity, reducing platform liability and regulatory risk.

Gaming

Biometric login and in-game purchase authentication protect player accounts from takeover, prevent unauthorized spending, and support age-assurance requirements at the point of action.

Social Networks

Account recovery, re-authentication after suspicious activity, and identity verification for monetisation or creator programmes ensure that accounts are controlled by their legitimate owners, reducing impersonation and platform abuse.

Ready to Strengthen Your Authentication?

Discover how Shufti Biometric Face Authentication helps you stop account takeover, reduce friction, and verify returning users, without disrupting the customer experience.

www.shufti.com
sales@shufti.com

Talk to an expert