



KAIZEN VOIZ

simple • seamless • secure

SIMPLIFY BANKING. AMPLIFY SECURITY.



A Practical Guide to
Securing Digital Banking
with **Kaizen Secure Voiz**

TABLE OF CONTENTS

- 🕒 Introduction: Biometrics in Banking
- 🕒 What is Face & Voice Recognition?
- 🕒 Why Banks Need It
- 🕒 How It Works (Simple Overview)
- 🕒 Quick Setup & Integration
- 🕒 Core Features for Banks
- 🕒 Smart Tools & Add-ons
- 🕒 Security & Compliance
- 🕒 Software Updates
- 🕒 Banking Case Studies
- 🕒 Conclusion: The Future of Secure
- 🕒 Banking
- 🕒 Glossary

INTRODUCTION: BIOMETRICS IN BANKING

Banking has always been built on trust and in today's digital-first world that trust is tested every second. Customers expect quick, secure access to their accounts from anywhere, whether it's through a mobile app, ATM or call center. At the same time, fraudsters are becoming more sophisticated, exploiting weaknesses in Passwords, Pins, OTPs and Physical ID checks.

Biometric technology, particularly face and voice recognition, is transforming how banks verify identities. Instead of relying on something a customer knows (like a password, Pins) or something they have (like a card), biometrics use something that are, unique physical and behavioral traits that cannot be easily stolen or faked.

For banks, this means faster onboarding, frictionless transactions & stronger fraud prevention. For customers, it means a seamless, password-free experience that feels natural and secure, all while meeting strict regulatory compliance standards.



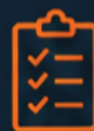
**STRONGER
SECURITY**



**FASTER
ONBOARDING**



**SEAMLESS
EXPERIENCE**



**REGULATORY
COMPLIANCE**



WHAT IS FACE & VOICE BIOMETRICS

Face and voice recognition are advanced biometric technologies that verify a person's identity using their unique physical and behavioral traits.

Face recognition works by capturing an image of the user's face and mapping key points, such as the distance between the eyes, shape of the jawline and contour of facial features, to create a secure "facial template." This template is compared against stored records to confirm identity.

Voice recognition analyzes the unique sound patterns in a person's speech. It goes beyond words, examining pitch, tone, accent, rhythm and even the shape of the vocal tract.

When used together, face and voice biometrics provide multi-layered authentication. For banks, this dual verification adds an extra shield against fraud while offering customers a quick, natural and contactless way to access services, whether they're at an ATM, using mobile banking or calling customer support.

WHY BANKS NEED IT

Banks operate in a high-stakes environment where security breaches can erode customer trust and cause significant financial loss. Traditional authentication methods, passwords, OTPs and physical IDs are increasingly vulnerable to phishing, SIM swaps and identity theft. As digital banking expands, the need for stronger yet frictionless security has never been greater.

This is where Kaizen Secure Voiz (KSV) delivers value. By combining face and voice recognition with liveness detection, KSV ensures that only real, verified customers can access accounts or authorize transactions. The system detects and blocks spoofing attempts like photos, deepfakes or recorded voices.

For banks, KSV digital banking solutions means faster eKYC, secure remote onboarding and safer high-value transactions. For customers, it offers a simple, password-free experience that works across mobile apps, ATMs and contact centers, all while meeting strict regulatory compliance. It's security that strengthens trust without slowing banking down.





HOW IT WORKS

Kaizen Secure Voiz (KSV) uses a multi-step yet seamless process to verify a customer's identity in seconds.

When a customer initiates a transaction, whether on a mobile app and call center, the system first captures their face via camera and/or records their voice. Advanced liveness detection ensures the input is from a real, present person and not a photo, video or recorded audio.

Next, KSV's AI-powered engine analyzes the facial features and vocal patterns, creating a biometric signature. This is securely matched against the bank's encrypted database.

If the match is successful, authentication is granted instantly.

From the customer's view, it's as simple as looking at a screen and speaking a phrase. For the bank, it's a robust, fraud-resistant process that quietly meets eKYC and compliance requirements while delivering speed and convenience.

QUICK SETUP & INTEGRATION

Kaizen Secure Voiz (KSV) is designed to fit seamlessly into a bank's existing infrastructure without disrupting daily operations. Deployment can be done on-cloud and on-premises, depending on the bank's compliance and security preferences.

Integration is achieved through secure APIs that connect KSV's biometric engine to mobile banking apps, ATM systems, internet banking portals and contact center platforms. This means banks can enable biometric authentication without overhauling their core systems.

The setup process typically involves configuring security policies, enrolling customer biometrics and training staff on usage and customer onboarding. With KSV's ready-to-use SDKs and multilingual voice capabilities, most banks can move from pilot to full-scale deployment in just weeks.

The result is a fast, low-friction rollout that delivers instant security upgrades and improved customer experience, without the heavy costs or long timelines of traditional system changes.



CORE FEATURES OF KSV DIGITAL BANKING SOLUTIONS

Modern banking demands a balance between top-tier security and a seamless customer experience. Kaizen Secure Voiz (KSV) is designed with this balance in mind, equipping banks with biometric technology that strengthens fraud prevention while making authentication fast and effortless for customers. Its capabilities are purpose-built to meet the operational needs, compliance standards, and scalability requirements of financial institutions.

PASSWORD LESS AUTHENTICATION

Enables secure logins and transaction approvals in seconds without PINs or passwords.



VOICE + FACE + LIVENESS DETECTION

Multi-layer verification to ensure the user is genuine, blocking spoofing and impersonation attempts.

PAPERLESS EKYC & REMOTE ONBOARDING

Allows customers to open accounts and complete verification without visiting a branch.



OMNICHANNEL COVERAGE

Works seamlessly across mobile apps, internet banking and contact centers.

ADVANCED SPOOF DETECTION

Detects and prevents fraud attempts using photos, videos or deepfakes in real time.



BUILT FOR BANKS OF ALL SIZES

Scalable and cost-effective for both large institutions and regional banks.

INDUSTRY APPLICATION OF KSV BIOMETRICS

While Kaizen Secure Voiz (KSV) is engineered with banking security as its primary focus, its advanced biometric capabilities extend to several high-security industries where identity verification is mission-critical

BANKING & FINANCE

Enables secure customer authentication for mobile and online banking, and high-value transaction approvals. KSV reduces fraud risk through multi-layer verification while delivering a seamless experience that strengthens customer trust.

INSURANCE

Supports remote policy onboarding, digital KYC, and claim verification without requiring physical presence. The proof-of-life feature adds a strong layer of security for large payouts, ensuring only the rightful policyholder is

TELECOM

Verifies customer identity during SIM card activation and service requests, preventing fraudulent activations and account takeovers. KSV also helps telecom providers meet stringent eKYC compliance requirements.

HEALTHCARE

Secures patient onboarding and grants controlled access to electronic medical records. With biometric verification, hospitals and clinics can meet HIPAA and ISO privacy standards while ensuring sensitive data stays protected.

KSV's adaptability, compliance-readiness and ease of integration make it a multi-industry solution that delivers both security and convenience.

SECURITY & COMPLIANCE

In banking, trust is earned through unwavering security and strict adherence to regulations. Kaizen Secure Voiz (KSV) is built on that promise, delivering industry-leading protection supported by verified credentials.

ISO/IEC 19795-2 Compliance

KSV's voice biometric solution has been independently tested by BixeLab (NIST/NVLAP-accredited), following ISO/IEC 19795-2 standards for facial & voice matching accuracy & performance.

International Recognition

Evaluations by BixeLab under NIST's NVLAP underscore KSV as one of the few providers whose biometric technology meets global security benchmarks.



ISO/IEC 19795-1 Compliance

The platform is also benchmarked against ISO/IEC 19795-1 norms for testing frameworks, further validating reliability under rigorous conditions.

ISO 19092:2023 Framework Alignment

KSV's architecture and biometric lifecycle, including enrollment, storage, transmission and authentication, align with ISO 19092's retail financial



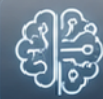
SOFTWARE

Kaizen Secure Voiz (KSV) is continuously enhanced to keep banks ahead of evolving security threats and customer expectations. Updates are delivered with minimal disruption, ensuring uninterrupted banking operations.

Regular AI model improvements boost the accuracy of face and voice matching, while liveness detection upgrades strengthen defenses against emerging spoofing techniques like deepfakes. Security patches are rolled out proactively to address new vulnerabilities before they can be exploited.

KSV also introduces feature enhancements through updates, such as new language packs for voice bots, expanded analytics capabilities and integration support for additional banking channels.

Banks receive clear release notes with every update, detailing changes and benefits, so IT and compliance teams can adapt quickly. Whether deployed on-cloud or on-premises, KSV ensures that the latest technology is always in place, keeping banking security both future-ready and regulation-compliant.



AI-Powered Accuracy

Continuous AI model improvements enhance face and voice matching accuracy and liveness detection.



Proactive Threat Protection

Regular security patches address vulnerabilities and protect against spoofing threats like deepfakes.



Feature Enhancements

New language packs, voice bot updates, analytics and channel integrations expand capabilities.



Seamless & Reliable Updates

Minimal disruption with clear release notes ensures uninterrupted banking operations.

BANKING CASE STUDIES

Case 1

Instant KYC Verification

A leading regional bank implemented KSV for real-time customer KYC during branch visits and remote onboarding. Verification time was reduced from hours to under two minutes, improving operational efficiency and enhancing the customer experience.



Case 2

Remote Account Opening

A mid-sized bank integrated Kaizen Secure Voiz (KSV) into its mobile banking app for eKYC. Customers could verify their identity using face and voice recognition without visiting a branch. Account opening time dropped from three days to under fifteen minutes, while fraudulent applications fell by 78%.



Case 3

High-Value Transaction Protection

A private bank enabled KSV re-authentication for transactions above ₹2 lakh. The additional biometric check reduced unauthorized high-value transfers to nearly zero, while maintaining a smooth customer experience.



CONCLUSION: THE FUTURE OF SECURE BANKING

Banking security is no longer just about locking systems, it's about creating trust through seamless, customer-first experiences. Kaizen Secure Voiz (KSV) combines face recognition, voice biometrics and liveness detection to offer banks a future-ready solution that is both highly secure and effortless for customers. By replacing passwords and PINs with unique biometric traits, KSV reduces fraud, speeds up transactions and meets strict regulatory standards.

As cyber threats evolve, banks that embrace such advanced authentication will stay ahead in both security and customer satisfaction. The future of banking belongs to those who make safety invisible yet powerful.



GLOSSARY

eKYC – Digital Know Your Customer verification.

- ✔ **LIVENESS DETECTION**
Ensuring a real person is present.
- ✔ **VOICEPRINT**
Digital model of vocal characteristics.
- ✔ **FACIAL TEMPLATE**
Encrypted map of facial features for matching.
- ✔ **AML (ANTI-MONEY LAUNDERING)**
Laws, regulations and procedures aimed at preventing criminals from disguising illegally obtained funds as legitimate income.
- ✔ **API (APPLICATION PROGRAMMING INTERFACE)**
A set of rules and protocols that allow different software applications to communicate with each other.
- ✔ **POA (PROOF OF ADDRESS)**
A document that confirms a person's residential address, used for verification in banking.
- ✔ **POI (PROOF OF IDENTITY)**
A document that verifies a person's identity, such as a passport or national ID.
- ✔ **SDK (SOFTWARE DEVELOPMENT KIT)**
A set of tools & resources that allows developers to integrate specific software functionalities into their applications.



**FOR INQUIRIES AND PARTNERSHIP
OPPORTUNITIES, REACH OUT TO US**



**LET'S
CONNECT**



**SCAN TO
EXPLORE**



KAIZEN VOIZ

simple · seamless · secure

Kaizen Secure Voiz pvt. Ltd.



**Registered Office: Plot No.26, 2nd Flr, Bhuvaneswari Nagar,
3rd Street, Velachary, Chennai- 600042**



044-22440091



www.kaizenvoiz.com