FORTANIXOR

SECURE. SMART

OUR CLIENTS

GovQ

Odentika

CredKin

JOYA

wellmoe

أرقام
arqaam

UBL
where you come first

HBL
MICROFINANCE BANK
مائیکروفنانس بینک

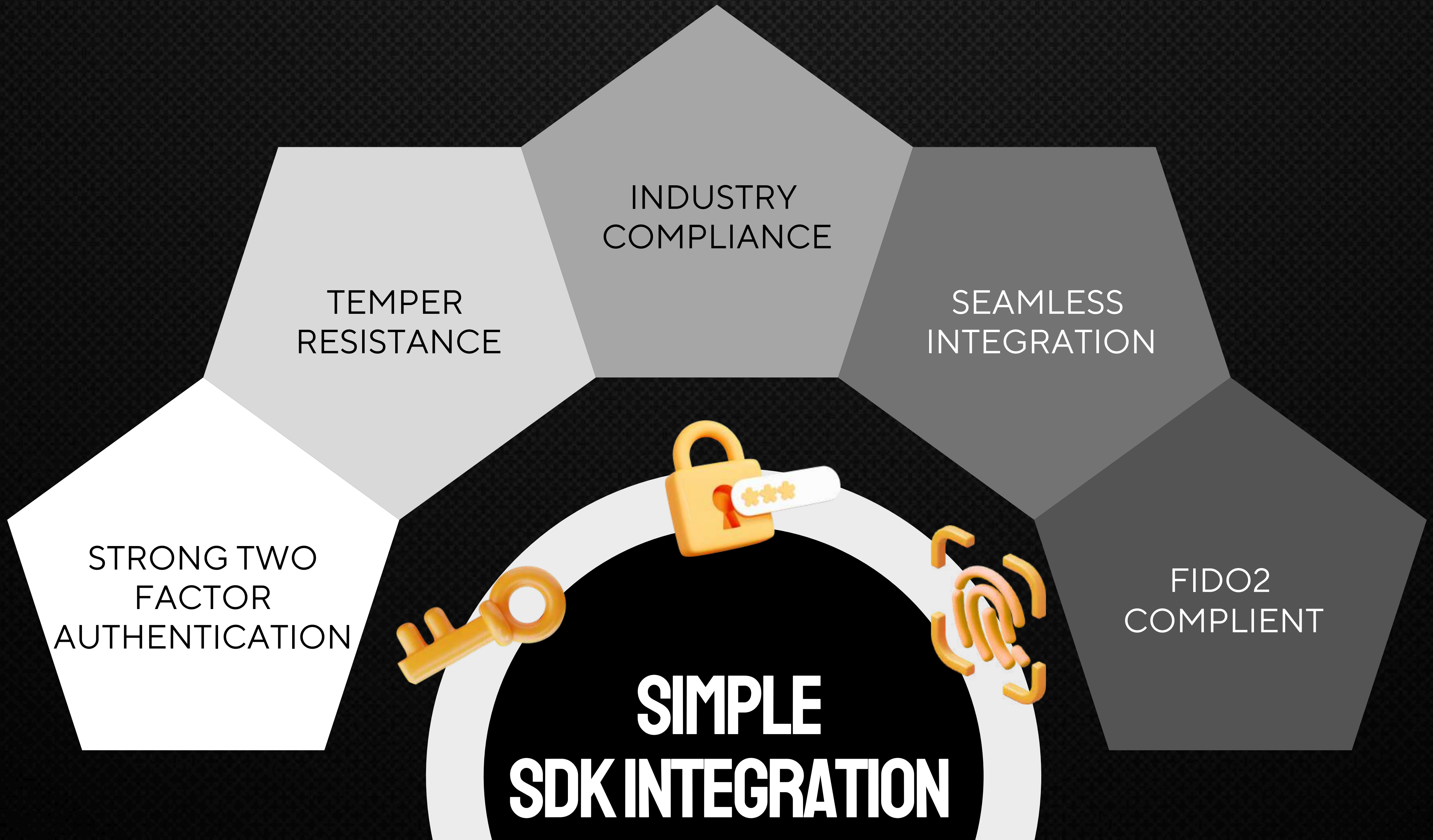
FortAuth™

Fortanixor delivers a complete FIDO-compliant platform for financial institutions and service providers to seamlessly meet CBUAE compliance for both mobile apps and web:

✅ FIDO2/WebAuthn SDKs for app & web
✅ Trusted Device Support
✅ Secure in-app authentication workflows
✅ Modular integration with existing banking platforms

SECURITY IN YOUR HANDS

SDK based solution, customisable for bank needs
Built to prevent extraction of private keys.



SECURING THE FINANCIAL APPS

Platform Authenticators
Leveraging Built-in Security

01

Integrated Devices

Huawei, iOS touch id, Android biometrics

02

Device Bound Keys

Keys protected by the OS security layers

03

Seamless Experience

Authenticate quickly using biometrics or PIN

04

Compliance

All devices compliant with FIDO 2

This authentication approach leverages device-native biometrics, secure key storage, and FIDO 2 compliance to deliver a seamless yet robust security experience.

HOW IT WORKS?

Platform Authenticators
Leveraging Built-in Security

TRIGGERS

- Signups
- Payment Authentications
- Add new payees
- Change in personal details
- Forget Password
- ... etc.

REGISTRATION

Device Mapping

Device creates key pair; public key sent to service.

CHALLENGE

Device Verification

Service sends a challenge to the user device.

RESPONSE

Device Locking

Device signs challenge with private key.

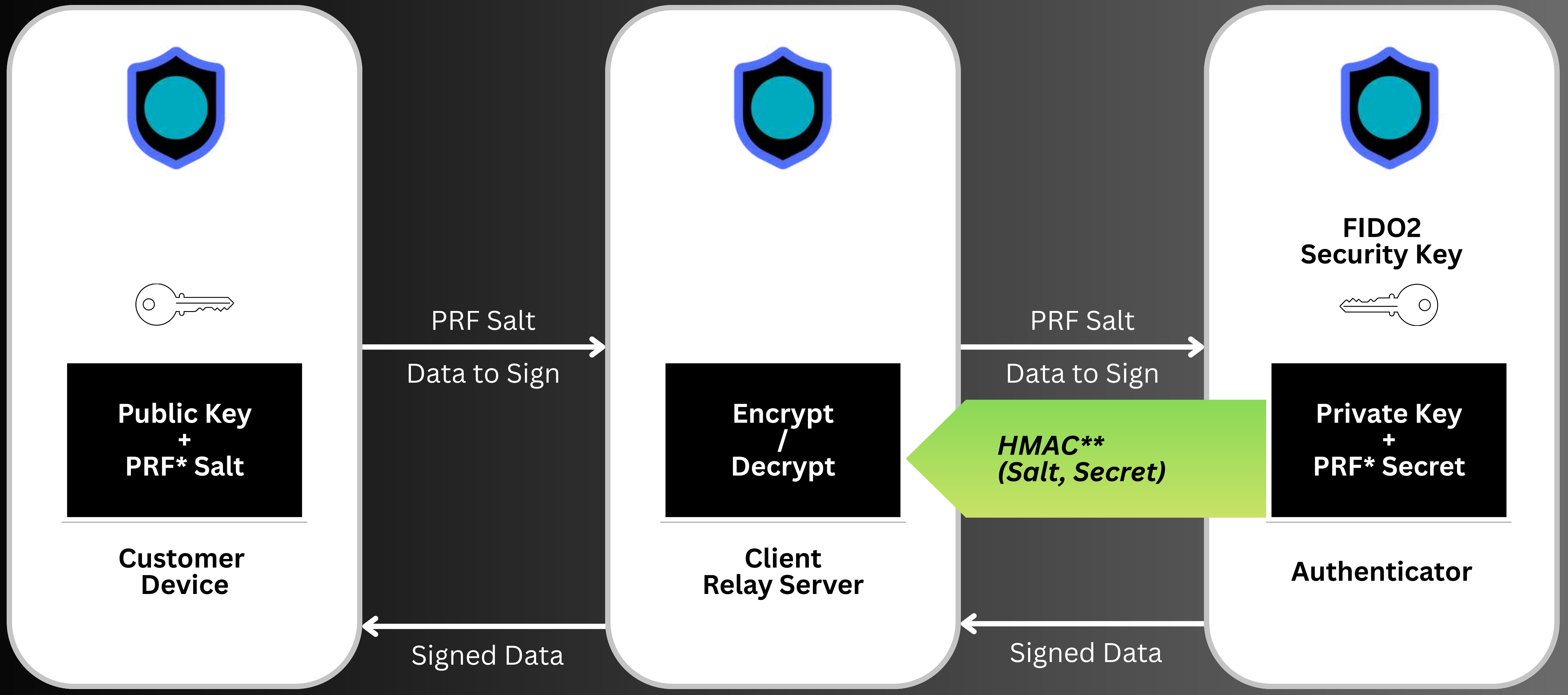
ACTION

Completion

Service verifies signature with stored public key.

TECHNICAL ARCHITECTURE

FortAuth™

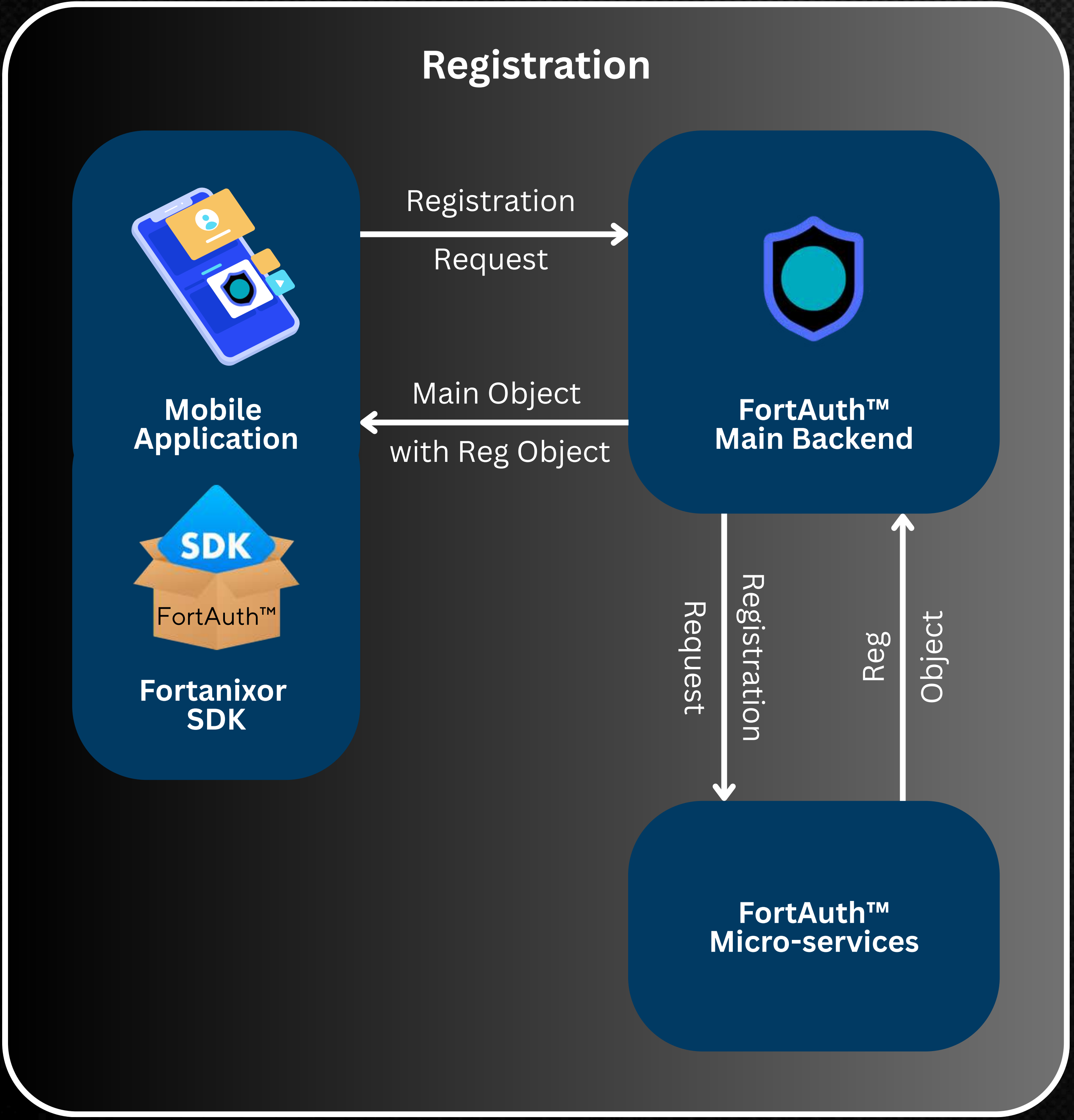


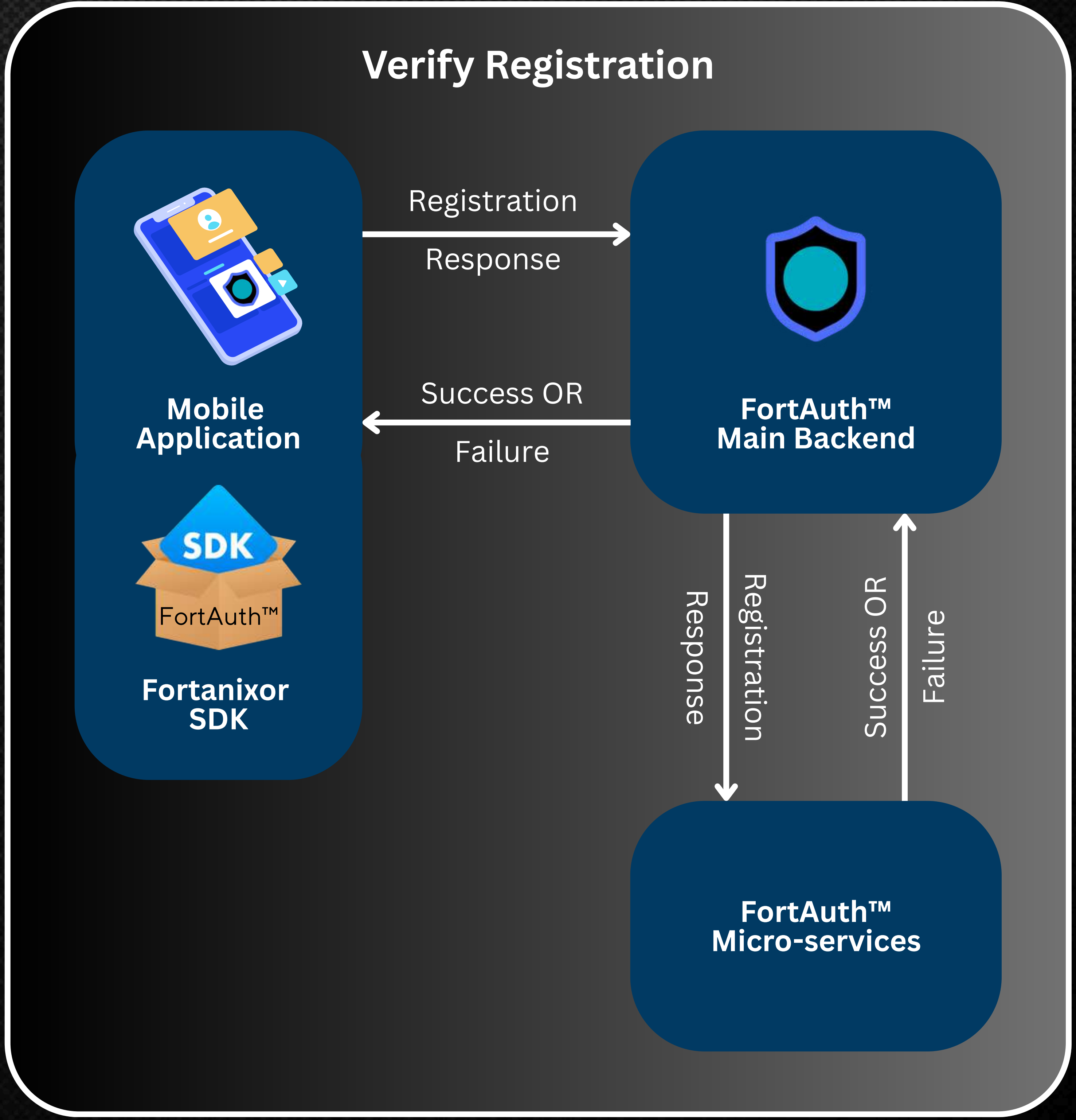
*PRF salt refers to a cryptographic salt value used in conjunction with a Pseudo-Random Function (PRF) extension, introduced to enable secure, application-specific secrets derived from a user's authentication credentials.

**HMAC salt" refers to the input value used with the PRF extension, where HMAC (Hash-based Message Authentication Code) is the underlying function used by the authenticator to generate a secure, deterministic output

TECHNICAL FLOWS 1/2

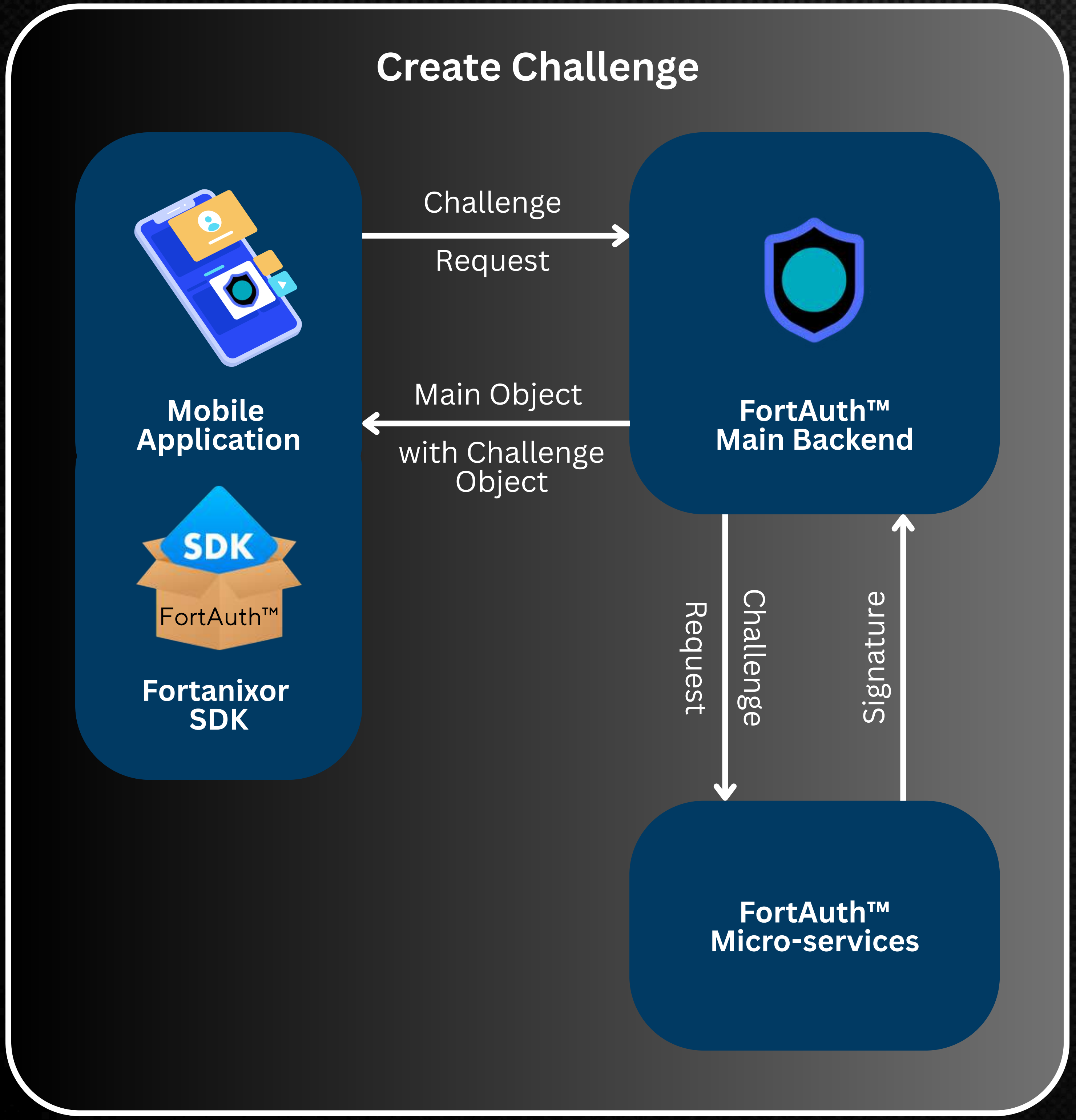
FortAuth™ - Registration Use Case

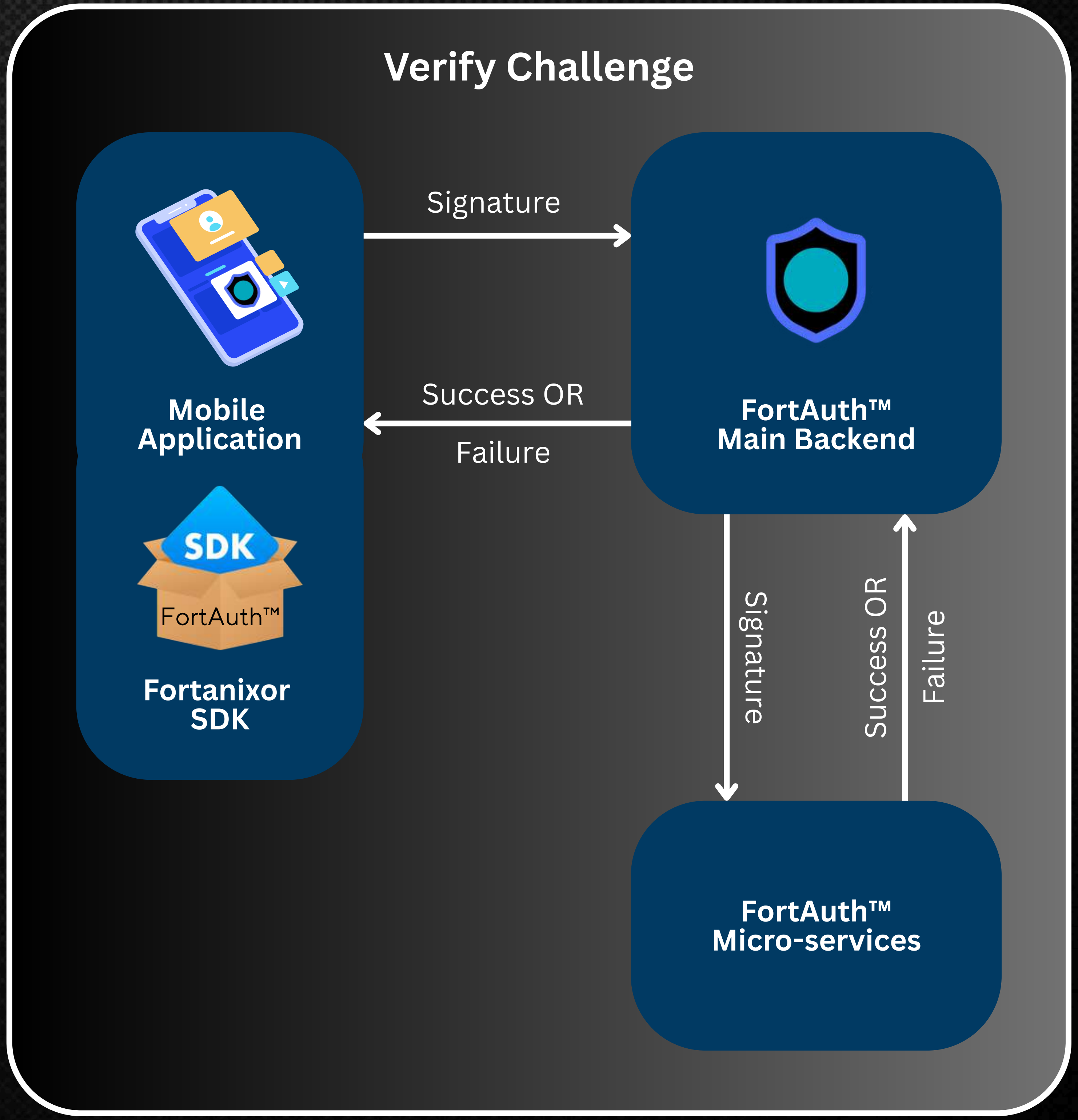




TECHNICAL FLOWS 2/2

FortAuth™ - Challenge Use Case





KEY BENEFITS

FortAuth™

Objective
Eliminate reliance on OTPs while reducing customer friction and improve authentication success rate.

How it will work?
FortAuth™ uses FIDO2-compliant, device-bound key pairs secured by biometrics or PIN to enable secure, passwordless access. When a customer registers, their device generates a key pair. For every login or transaction, the system sends a cryptographic challenge which the device signs using its private key. The backend verifies this using the stored public key—removing the need for OTPs or passwords.

Desired customer behavior
FortAuth™ aims to improve authentication success rates, lower helpdesk volumes, and enhance user trust through frictionless security. The result is a secure, phishing-resistant experience that encourages higher digital adoption and reinforces Banks position as a leader in secure, customer-centric banking.

Reduced Support

Fewer password resets and help desk calls.

Enhanced Security

Phishing-resistant, no shared secrets.

Channel Choice

Broadreach media in non-traditional environments

User Friendly

Fast, convenient, passwordless login

EXPECTED BUSINESS IMPACT

FortAuth™: Leveraging Built-in Security

01

Drop in login failure rates due to passwordless flow.

By eliminating OTPs and passwords, FortAuth™ reduces common failure points in authentication. Users can log in with device-native biometrics or PIN, minimizing friction and boosting success rates—especially in low-connectivity environments.

02

Increase in successful onboarding through seamless verification.

With one-touch mobile number verification and biometric authentication, the onboarding journey becomes frictionless and intuitive. This drives higher completion rates and reduces abandonment during account setup.

03

Reduction in helpdesk calls related to password or OTP issues

Password resets and OTP failures are among the top drivers of support queries. By replacing these with secure device-bound keys, FortAuth™ significantly cuts down inbound support traffic and operational overhead.

04

Higher customer satisfaction and app ratings driven by ease of use and security.

Customers prefer experiences that are both convenient and secure. FortAuth™ delivers on both fronts, enhancing overall satisfaction and boosting app store ratings through a modern, trust-centric login experience.

CLONE DETECTION DEMO

Fortanixor

Test (Before SDK):
We cloned the OS of Device A onto Device B.
Banking app worked on Device B because all app data & IDs were copied.
The system couldn't tell it's a clone — no hardware-level validation.

After Fortanixor SDK Integration:
SDK binds a secure key to the phone's hardware (TEE).
During login, the app sends a challenge to be signed using that key.
Original Device A signs and authenticates.
Cloned Device B fails — the key doesn't exist in its hardware.ardware trust

Result:
Cloned device gets blocked.
No need for IMEI, Android ID, or basic fingerprinting.
Validation is based on uncloneable hardware trust.

IMPLEMENTATION PLAN

FortAuth™: Leveraging Built-in Security

Week 1 Planning & FIDO2 Requirements

Define objectives, stakeholders, and FIDO2 integration needs.

Week 2 Technical Design & Architecture

Design backend and app integration for FIDO2 (WebAuth)

Week 3 - 4 Development & Integration

Implement FIDO2 (biometrics/security keys) and fallback methods

Week 5 - 6 QA & Deployment

Security audits, compatibility, user testing, Release app update and monitor usage

PREMIUM FIDO-BASED SECURITY SOLUTION

Value Justification

Category	Value Driver	Business Impact
🔒 **Authentication Security**	**FIDO2/WebAuthn**	Phishing-resistant, passwordless login; eliminates credential-based attacks
📲 **MSISDN Intelligence**	**Real-time SIM verification**	Prevents SIM swap, enhances mobile identity assurance
🧠 **R&D Investment**	**Proprietary mobile SDKs, backend cryptographic protocols**	Constantly evolving; optimised for financial industry and mobile-first ecosystems
👩‍💻 **Resource Upskilling**	**Specialized training in FIDO, mobile app security, attestation**	Deep technical expertise; reduced dependency on external consultants
🚀 **Scalability**	**Built for high concurrency, multi-region deployment**	Enterprise-ready performance and availability
🛠️ **Tooling & Infra**	**CI/CD, telco compatibility, Secure Coding practices**	Robust, scalable, and high-assurance environment
💸 **Cost Efficiency**	**Lower TCO than SMS OTP**	Saves recurring SMS gateway costs; no OTP delivery failures or latency

FORTVOICEAGENT™

AI Call Center

FORTVOICEAGENT™

AI Call Center

Revolutionising call centers with AI-driven automation.
Deployed across U.S. & KSA in multiple industries.
Tailored for the Banking Sector: secure, multilingual, compliant, and scalable.

Proven Success Stories

28 Dental Clinics (U.S.)
Seamless booking & patient engagement.

GovQ Startup (U.S.)
AI-driven citizen query management.

JOYA Apps (KSA)
AI-enabled social commerce & gifting platform.

FORTVOICEAGENT™

Multilingual Advantage

Languages Supported:

- English
- Arabic (Najdi Dialect)
- Spanish (Puerto Rican, Esanglish, African-American)
- Urdu 🇵🇰

Regional Language for Pakistani Market:

- Sindhi
- Punjabi
- Siraiki
- Pashto
- Balochi

FORTVOICEAGENT™

Core Capabilities

Scalable AI Models
Adapt to regional dialects & accents.

Framework for Fine-Tuning
Custom banking use cases.

Configurable Settings
Voice, accent, empathy level, APIs.

Smart Tool Calling
Connects directly with banking systems.

Built-in FIDO2 Security Layer
Ensures safe customer authentication.

FORTVOICEAGENT™

Dashboard & Monitoring

KPIs Tracked in Real-Time

Success Rate
Avg. Empathy Score
Avg. Response Time
Recent Issues
Avg. KPI Score

Agent Health (AI Agent KPIs)

Intent Recognition
Task Completion
Empathy Score
Dialogue Flow
Branch Logic Accuracy
Entity Extraction Accuracy

Technical Performance

Response Latency
System Uptime
API Response Time
Call Drop Rate
Call Initiation Time
Speech Clarity (TTS)
Transcription Accuracy
Call Recording
Fallback Rate

Conversational Quality

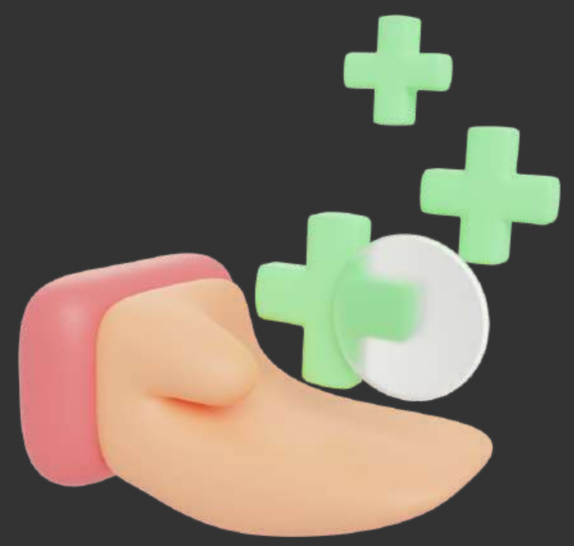
Interrupt Handling
Turn-Taking Management
Multi-turn Memory Recall
Context Retention
Tone Appropriateness
Accent Understanding
Disfluency Handling

FORTVOICEAGENT™

Usecase & Benefits

Banking Use Cases

24/7 Customer Support
Balance & Transaction Queries
Credit Card Requests
Credit Card/Debit Card Block/Unblock
Loan Application Assistance
Fraud Detection Alerts



Benefits for Banks

Lower Call Center Operational Costs.
Faster Response & Resolution.
Human-like Customer Experience.
Secure, password-less user authentication.
Local & global languages.
Real-time monitoring
Compliance assurance

VOICEAUTH™

Digital Banking

VOICEAUTH™

Digital Banking

Current Challenges in Digital Banking

- Too many taps & clicks → poor user experience.
- Complex app menus confuse users.
- Accessibility gaps for non-tech-savvy and regional language speakers.
- Rising need for secure, compliant authentication.

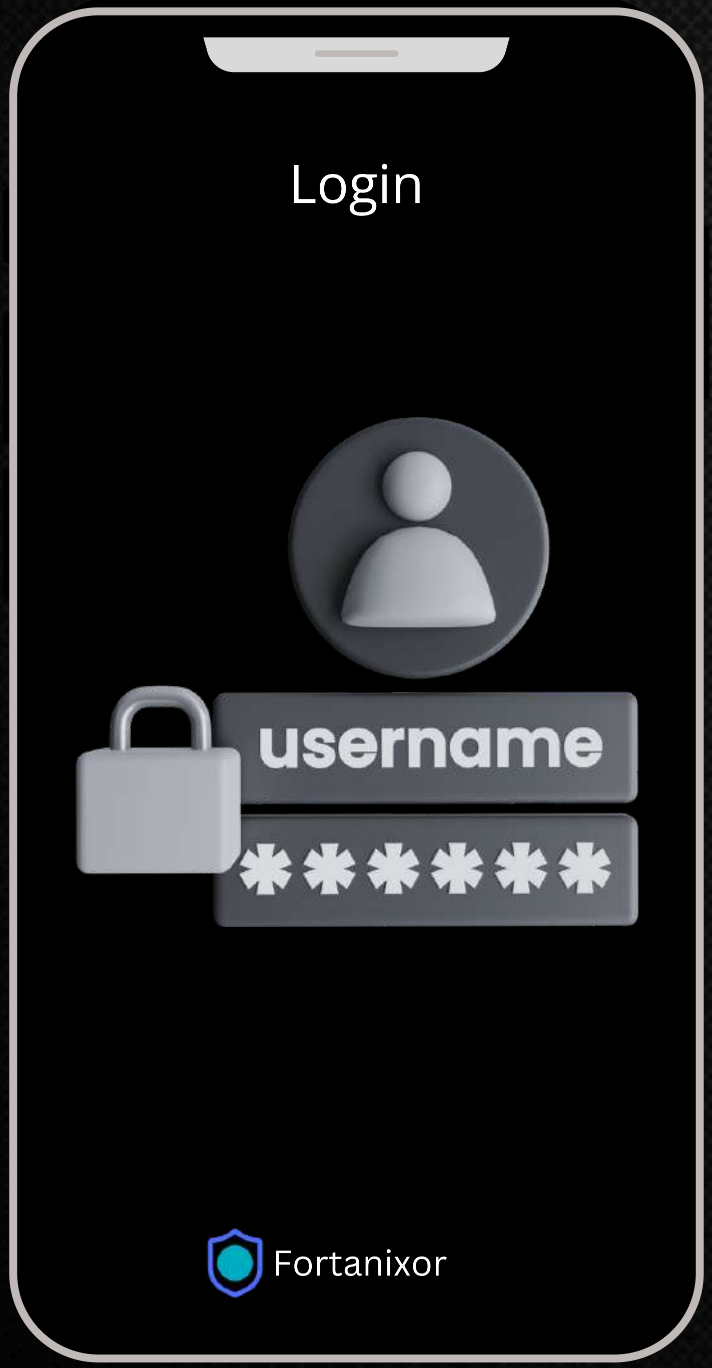
VOICEAUTH™

Value Proposition

VoiceAuth™ delivers...

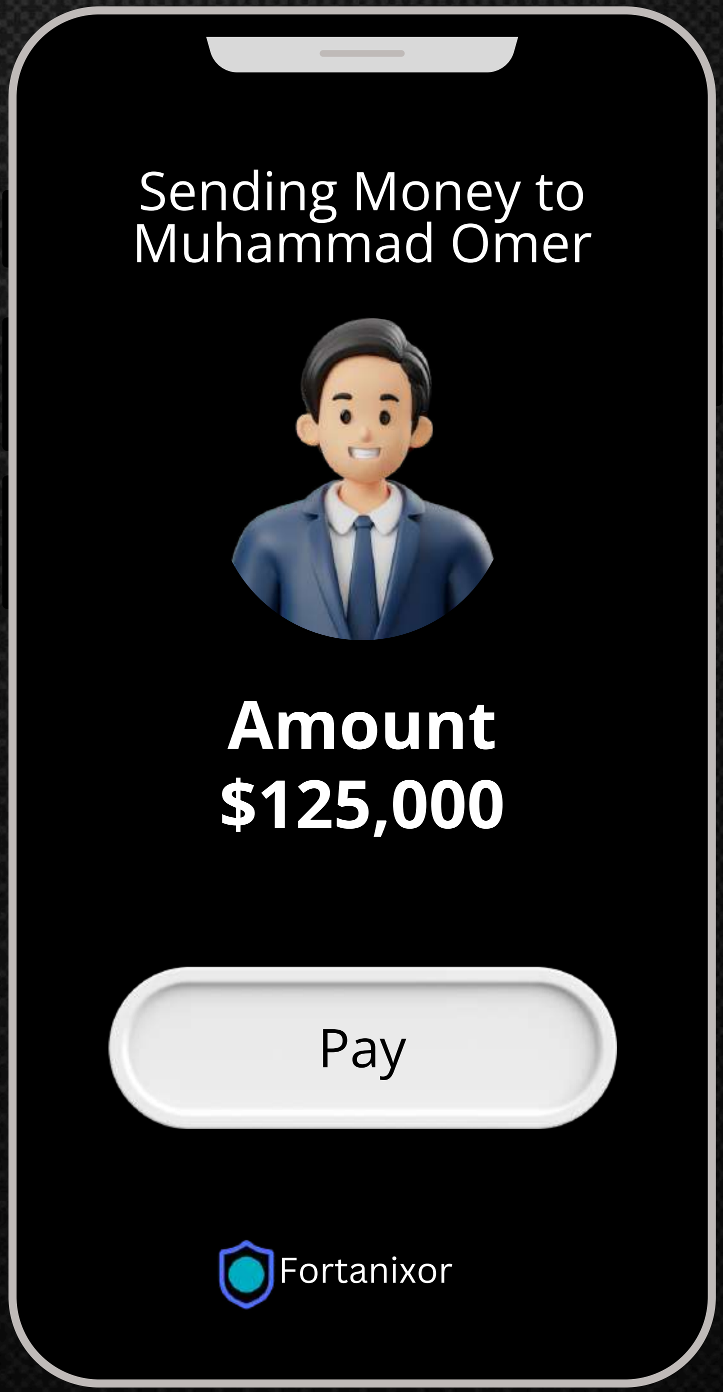
- 🎯 **Frictionless Journeys** → Customers complete tasks with a single voice command, reducing clicks and navigation pain.
- 🌍 **Inclusive Banking** → Regional language & dialect support expands access to underserved segments.
- ⚡ **Operational Efficiency** → Cuts support queries, lowers handling costs, and simplifies customer service.
- 🚀 **Future-Ready Experience** → Conversational AI transforms mobile banking into an intuitive, human-like assistant.
- 🔐 **Secure by Design (backed by ForthAuth™)** → FIDO2-compliant authentication using device lock ensures strong, phishing-resistant security.

VOICEAUTH™

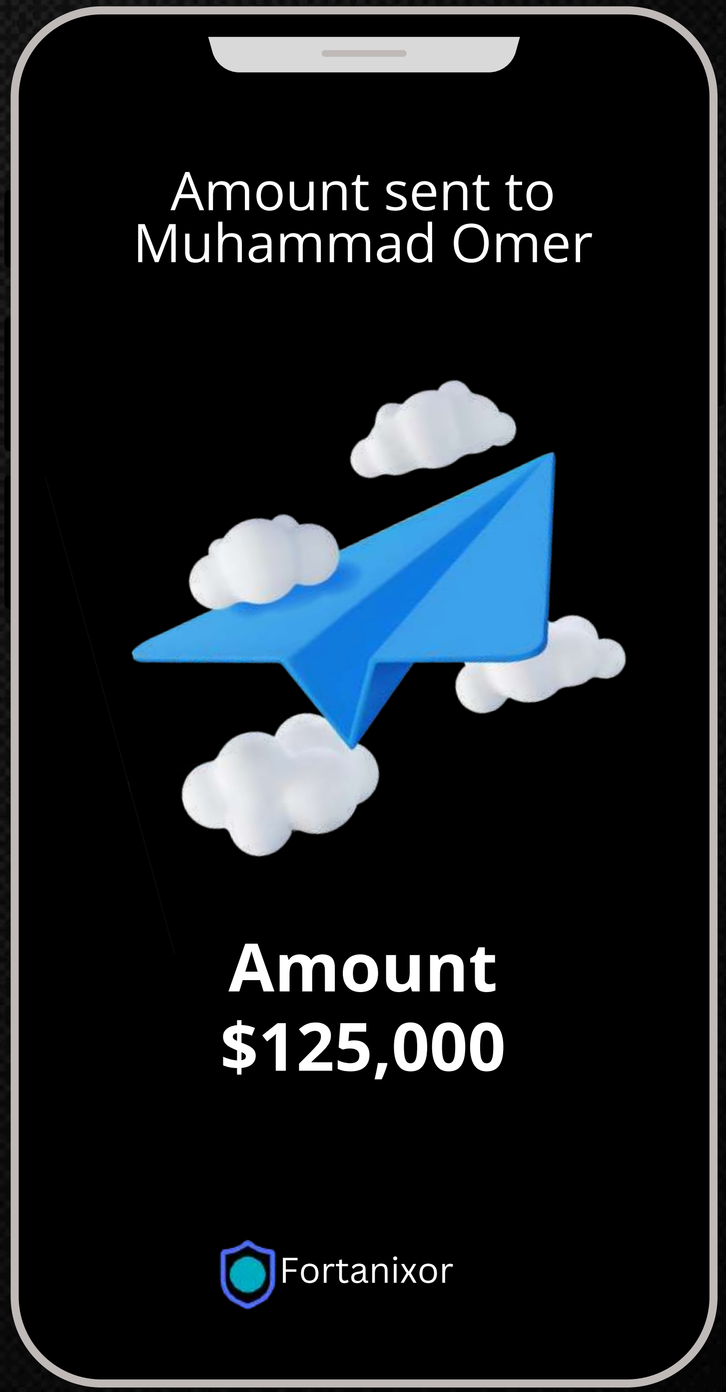


Customer opens banking mobile application

Customer simply says: "Transfer $125,000 to Muhammad Omer"



App instantly generates transaction details. User reviews the details & confirm.



Transaction processed securely & instantly

VOICEAUTH™

Impact for Banks & Customers

- 🚀 **Superior Experience** → Simpler journeys, higher app adoption.
- 🔐 **Trusted Security** → Backed by global FIDO2 standards.
- 🌍 **Inclusivity** → Broader reach via local languages.
- 📉 **Reduced Support Calls** → Customers self-serve via voice commands.
- 📈 **Innovation Edge** → Positions the bank as an AI-first industry leader.

"Reimagining Banking Customer Experience with AI + Security"
Your Partner in Innovation, Security, and Customer Delight.

AuthCash™

Unlock Cash. No Cards. No PINs. Only You

AUTHCASH™

Value Proposition

Instant, ultra-secure cash withdrawals—no card, no password, no OTP. Simply scan and authenticate with your device.

The Solution:

- No card, no PIN, no OTP
- Authenticate with; Biometrics (face/fingerprint/Lock pattern) via mobile banking application.
- ATM communicates securely with the bank’s FIDO2 server via mobile banking application.
- Transaction completed instantly after biometric verification

AUTHCASH™

The User Journey

Customer opens the Bank App and scans a QR code displayed at the ATM

The app triggers a secure FIDO2 authentication—via fingerprint, facial recognition, or a security key.

Upon successful authentication, the ATM dispenses cash, and the account is debited instantly.

AUTHCASH™

Key Advantages

Feature	ATM PIN (Traditional)	AUTHCASH - FIDO2 (Password-less Authentication)
Security Strength	Vulnerable to skimming, shoulder surfing, brute-force attempts. PINs can be stolen, guessed, or shared.	Resistant to phishing, skimming, replay, and brute-force. Private keys never leave device. Authentication is cryptographic.
User Experience	Requires remembering and typing a 4–6 digit PIN, which can be forgotten, mistyped, or exposed.	Seamless biometric (fingerprint, face) or device PIN. No memory burden, faster than typing.
Fraud Resistance	PINs can be compromised via card cloning, hidden cameras, malware-infected ATMs.	Authentication tied to the device + user biometrics. Even if device is stolen, biometric is required—making it nearly impossible to spoof.
Operational Cost	Banks must maintain ATM PIN infrastructure, fraud monitoring, and card replacement costs.	Lower fraud-related losses and reduced support costs (no “forgot PIN” cases). Eliminates dependency on card networks.
Privacy	PIN entered on a keypad, exposed to cameras or malicious overlays.	Biometric/PIN never leaves the device, not transmitted or stored centrally.
Compliance & Future-Readiness	Legacy method, less aligned with modern strong customer authentication standards (PSD2, NIST, etc.).	Built for regulatory compliance (PSD2 SCA, GDPR) and interoperable with passkeys, browsers, and mobile ecosystems.
Convenience	Requires physical ATM card + PIN entry.	Requires only a mobile device (QR + biometric)—no card, no PIN.

LET'S CREATE BANKING SECURE!

FORTAUTH™ ISN'T JUST A SECURITY LAYER – IT'S A STRATEGIC ASSET.

'THE TRUST ENGINE BEHIND SECURE AND SEAMLESS DIGITAL BANKING.

WRITE TO US:
HELLO@FORTANIXOR.COM

THANK YOU