

INVESTOR PITCH DECK

FortAuth: device-bound security for the next era of digital banking.

A FIDO2-based authentication and transaction approval platform built for banks, financial institutions, wallets, fintechs, and government digital services.

4M+**Customer traction**

Banking-scale usage footprint

5,000**TPS achieved**

High-volume performance test

FIDO2**Certification support**

Roadmap-ready architecture

**FORTANIXOR**

SECURE. SMART.

THE PROBLEM

Digital banking has outgrown OTP-based security.

Fraud has moved from simple credential theft to device compromise, remote control, screen sharing, social engineering, SIM abuse, and fake approval journeys.

1 Weak verification

SMS OTP, TPIN, and basic 2FA can still be phished, replayed, intercepted, or socially engineered.

2 Expensive at scale

Large banks spend heavily every month on OTP messages, alerts, and manual call confirmations.

3 Friction for users

Waiting for OTPs, failed messages, and manual checks create a poor customer experience.

Fraud attempts increase

OTP friction and recurring cost

Customer trust leakage

FortAuth closes the gap with device-bound approval

Legacy authentication creates a gap between convenience, cost, and security.

THE SOLUTION

FortAuth binds trust to the customer's device.

FortAuth turns the mobile app into a trusted security channel using FIDO2-style cryptographic authentication, device integrity checks, and contextual transaction approvals.

01

Customer Device

Private key remains on device



02

FortAuth SDK

Biometric / PIN / passcode approval



03

Risk Controls

Screen, call, SIM, root, emulator checks



04

Bank Core

Signed assertion and audit trail

A

Stronger authentication

Device-bound cryptography reduces phishing and OTP dependency.

B

Contextual approval

Users see transaction details before approving sensitive actions.

C

Lower recurring cost

High-volume flows shift from SMS/calls to secure in-app approvals.

PRODUCT

Feature stack built for real banking risk.

FortAuth combines authentication, transaction approval, device security, and mobile fraud defense in one platform.

Authentication

FIDO2 / Device-Bound Authentication

Trusted device enrollment

Biometric / PIN / passcode approval

Fraud Controls

Screen sharing blocker

Screenshot blocker

Live call detection - Cellular + WhatsApp

Device Intelligence

SIM verification - Android only

Emulator / simulator detection

Rooted / jailbreak device detection

Transaction Layer

SSL pinning

In-app notifications

3DS transaction approval

Login

FIDO2 + device trust

Enroll

Trusted device model

Approve

Contextual transaction approval

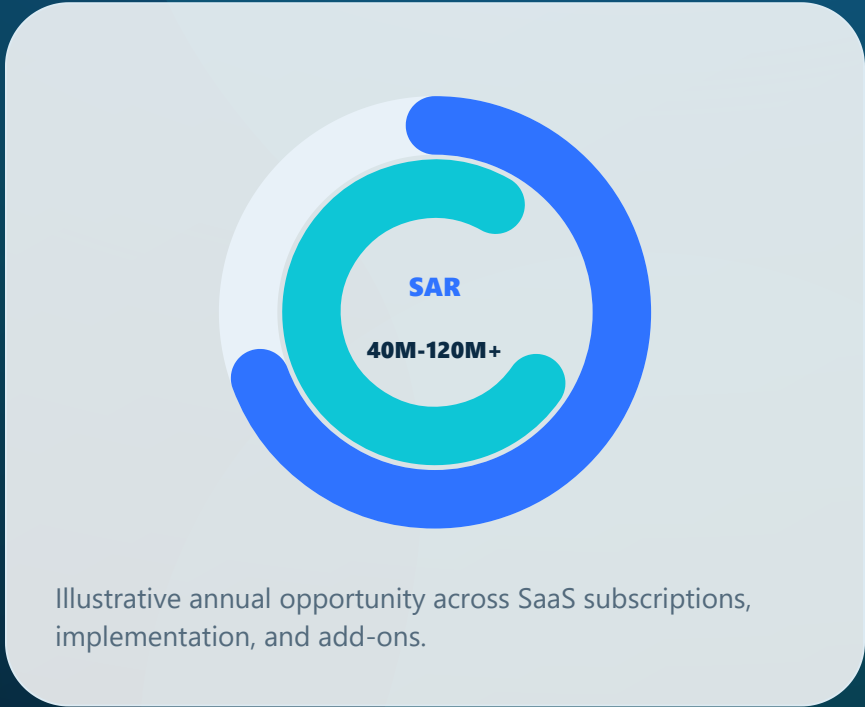
Protect

Anti-fraud add-ons

MARKET

Saudi Arabia and MENA are ready for stronger authentication.

Banks, fintechs, wallets, payment companies, brokerages, and government digital services need secure mobile approval flows with lower OTP dependence.



Planning estimate only. Exact market size depends on target accounts, pricing, deployment model, and adoption velocity.

SAUDI MARKET SIZE

Saudi Arabia gives FortAuth a 400+ target financial-sector universe.

The KSA market includes banks, fintechs, payment providers, finance companies, insurance players, and capital-market institutions that all need stronger login, transaction approval, and fraud-resistant customer authentication.



Sources referenced in the market model: Saudi Press Agency / SAMA, Argaam fintech data, Saudi Central Bank payment provider licensing, Arab News finance company licensing, and Milliman Saudi insurance market update. Pricing model based on FortAuth commercial assumption: \$1M/year for 20M users and 50M monthly transactions.

SERVICEABLE AVAILABLE MARKET

Near-term KSA SAM: \$20M–35M ARR from high-fit regulated buyers.

FortAuth should first focus on institutions where authentication cost, fraud exposure, compliance pressure, and customer-scale are already board-level issues.

SEGMENT	BUYER COUNT	FORTAUTH OPPORTUNITY	ARR POTENTIAL
Major banks	39 licensed banks	Highest-value priority accounts; 10 major banks at ~\$1M ARR each.	\$10M
FinTech companies	301 companies	10%–15% adoption at smaller pricing for wallet login and transaction approval.	\$5M–15M
Payment providers	32 licensed PSPs	Payment authorization, app login, fraud reduction, and secure approval flows.	\$3M–8M
Finance / BNPL / lending	74 finance companies	Customer verification, loan approvals, mandates, and high-risk digital actions.	\$4M–10M
Insurance / capital market	26+ insurers + CMA ecosystem	Secure login, policy approval, investment transactions, and profile changes.	\$3M–7M
Serviceable market	Focused regulated buyers	Prioritized by budget, urgency, integration fit, and enterprise buying capacity.	\$20M–35M ARR

NEAR-TERM SAM

\$20M–35M

Practical revenue pool after prioritizing high-scale institutions, regulated buyers, and customers that can adopt FortAuth first.

Sales focus

Start with banks and payment providers, then expand to fintech, BNPL, lending, insurance, and CMA-regulated institutions through reference deployments and integration partners.

SERVICEABLE OBTAINABLE MARKET

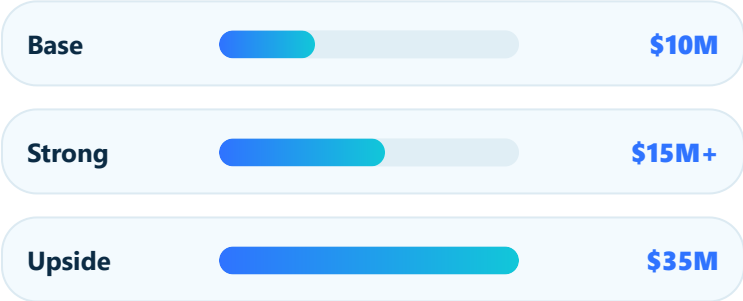
FortAuth can target \$10M ARR in KSA with only 10 major institutions.

The initial obtainable market does not require broad market capture. A focused enterprise motion toward 10 major institutions creates a meaningful recurring ARR base, with upside from fintech, PSP, and lending expansion.

CORE SOM TARGET

\$10M

10 major KSA institutions × \$1M annual FortAuth license.



YEAR 1

Land 2–3 anchor institutions

Use Saudi banking urgency, FIDO2 certification, and cost-reduction narrative to close first enterprise deployments.

\$2M–3M ARR

YEAR 2

Expand to 5–7 regulated customers

Convert references into PSP, fintech, BNPL, and finance company sales through partner-led implementation.

\$5M–7M ARR

YEAR 3

Reach 10–12 major customers

Establish FortAuth as the trusted approval layer for high-risk digital financial actions in Saudi Arabia.

\$10M–12M+ ARR

SAUDI MARKET SIGNAL

Al Rajhi CDO meeting insights confirm a stronger-authentication roadmap.

Based on last week's FortAuth discussion with the Al Rajhi Chief Digital Officer, Al Rajhi is still using OTP in relevant digital banking journeys. This creates a practical path to shift from OTP-based confirmation to device-bound, FIDO2-grade approval.

INSIGHT 01

OTP is currently used

The recent CDO discussion confirmed that OTP still exists in Al Rajhi's digital journeys. FortAuth should be positioned as a safer upgrade path, not only as a cost-saving tool.

INSIGHT 02

FIDO2 is already on the roadmap

The discussion indicated that Al Rajhi has explored FIDO2-style authentication and is closely aligned with SAMA's stronger-authentication direction.

INSIGHT 03

High-value approvals are the entry point

The strongest pitch is for transaction approvals, beneficiary actions, device enrollment, 3DS flows, and fraud-sensitive mobile journeys.

INSIGHT 04

FortAuth angle

Position FortAuth as a certified, implementation-ready FIDO2 layer that reduces OTP dependency while improving security, auditability, and customer experience.

Internal meeting insight from the recent FortAuth pitch conversation with Al Rajhi CDO. Validate exact external wording before public circulation.

COST OPPORTUNITY

OTP, transaction alerts, and confirmation flows create a measurable AI Rajhi cost-reduction opportunity.

Based on the meeting assumption: 40M login OTP messages per month and 50M transaction alerts per month. The estimate below uses SAR 0.05 - 0.08 per SMS plus call-confirmation handling costs.

40M

Login OTP / month

Recent meeting insight

50M

Transaction alerts / month

Monthly alert volume

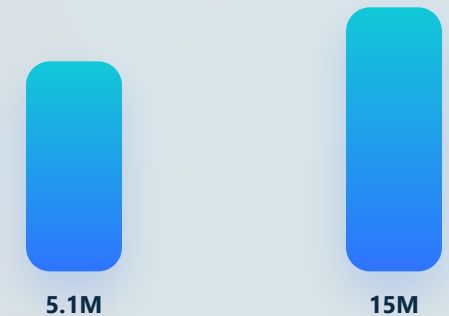
SAR 4.9M - 10.2M

Estimated monthly exposure

SMS + call confirmation

COST AREA	VOLUME BASIS	COST LOGIC	MONTHLY EXPOSURE
OTP Authentication	20M Transactions / month	20M x SAR 0.01 - 0.03 / SMS	SAR 200K - 600K
Transaction Alerts	20M transaction alerts / month	20M x SAR 0.01 - 0.03 / SMS	SAR 200K - 600K
Beneficiary Addition Alerts	250K - 500K sensitive events	SAR 0.01 - 0.03 / SMS	SAR 2,500 - 5,000
Call for Confirmation	250K - 500K high-risk calls	Estimated SAR 0.10 / handled call	SAR 25,000 - 50,000
Total Estimated Exposure	40.5M+ SMS events + calls	OTP + alerts + sensitive-action controls	SAR 427K - 1.25M / month
Total Estimated Exposure (Yearly)	486M+ SMS events + calls	OTP + alerts + sensitive-action controls	SAR 5.1M - 15M / Year

Recalculated exposure



SAR 5.1M - 15M / Year

Estimate uses 486M+ OTPs, transaction alerts, beneficiary alerts, and call-confirmation handling. Exact AI Rajhi costs are not publicly disclosed.

TRACTION

FortAuth enters the market with proof points and a credible banking pipeline.

UBL + HBL

Existing customer references
Banking engagement proof

4M+

Customer traction
Validated footprint

5,000 TPS

Achieved throughput
Performance readiness

FIDO2 Cert

Cybersecurity validation
Certification evidence

Pipeline and target institutions

ABL

Meezan Bank

Bank Makramah

Mashreq Bank

Faysal Bank

EasyPaisa

Mobilink Bank

Askari Bank

National Bank

Al Baraka Bank

Pipeline strength: multiple banking and FI conversations across Pakistan, Saudi Arabia, UAE, and MENA.

COMPETITIVE LANDSCAPE

FortAuth wins by combining FIDO2 with bank-specific mobile fraud controls.

CAPABILITY	FORTAUTH	NOK NOK	NEVIS	ONESPAN	HID GLOBAL
FIDO2 / Passkey foundation	Strong	Strong	Strong	Strong	Strong
Mobile banking fraud add-ons	Deep stack	Limited	Moderate	Strong	Moderate
Regional deployment agility	High	Enterprise pace	Enterprise pace	Enterprise pace	Enterprise pace
Transaction approval context	Strong	Strong	Strong	Strong	Moderate
SaaS + implementation flexibility	High	Medium	Medium	Medium	Medium



CERTIFICATION & TRUST

Fortanixor’s FIDO2 certification strengthens enterprise buyer confidence.

Fortanixor has FIDO2 Server Certification for FortAuth FIDO2 Server. This strengthens procurement, InfoSec, audit, and regulatory discussions with banks and financial institutions.

01

FIDO2 Server certified

Fortanixor's FortAuth FIDO2 Server is certified for FIDO2 Specification Version 2.1 with Server implementation class.

02

Buyer confidence

The certificate gives banks a stronger evidence base during procurement, InfoSec review, and technical due diligence.

03

Implementation readiness

SDK guides, API flows, security controls, deployment diagrams, and response material help reduce bank onboarding friction.

04

Compliance alignment

FIDO2 certification supports stronger authentication language for regulated banking, payment, and government digital services.



Fortanixor FortAuth FIDO2 Server Certification - Specification Version 2.1, Implementation Class: Server, Issued August 06, 2025.

BUSINESS MODEL

Recurring SaaS with enterprise implementation revenue.

Base SaaS Subscription

Annual platform license for authentication, trusted-device management, audit trail, policy control, and reporting.

Usage / Scale Tier

Expansion by MAU, TPS, transaction approvals, active devices, or bank-agreed volume tiers.

Enterprise Implementation

One-time setup, SDK integration, backend integration, security testing, deployment support, and rollout governance.

Security Add-ons

Fraud controls, 3DS approval, in-app notifications, device intelligence, and high-risk action orchestration.

The model grows with the bank: start with core authentication, expand into transaction approvals, add fraud controls, then scale with customer and transaction volume.

Recurring Base SaaS renewals	Expansion Usage and add-ons	Services Implementation revenue
--	---------------------------------------	---



GO-TO-MARKET

Focused enterprise sales into high-value regulated buyers.

Tier-1 Banks

Replace OTP dependency, secure device enrollment, and approve high-value transactions.

Primary buyer:

CIO, CISO, Digital Banking, Fraud Risk

Wallets & Fintechs

Secure fast-growth mobile platforms while reducing fraud and support load.

Primary buyer:

CTO, Risk, Product, Compliance

Government Identity

Citizen authentication, e-service approval, and secure mobile app access.

Primary buyer:

Digital transformation, security, procurement

Payment & 3DS

Contextual approval for card, transfer, beneficiary, and high-risk actions.

Primary buyer:

Payments, cards, fraud operations

Reference wins

Paid pilots

Annual SaaS

Regional expansion

INVESTMENT CASE

FortAuth is positioned at the intersection of security, compliance, and cost reduction.

Why now?

OTP costs are high, fraud is more sophisticated, and regulators are pushing stronger digital trust.

Why FortAuth?

FIDO2 foundation plus mobile fraud add-ons, banking traction, 5,000 TPS performance, and SaaS scalability.

Why investors?

Capital accelerates certification, regional sales, implementation capacity, and enterprise credibility.

Use of funds



- Certification + Product
- Saudi/MENA GTM
- Delivery + Documentation



FortAuth can become the trusted approval layer for digital banking in MENA.

Secure. Smart. Built for banks, financial institutions, fintechs, and government digital services.

WEBSITE

fortanixor.com

EMAIL

hello@fortanixor.com

PHONE

+971 505 460 852