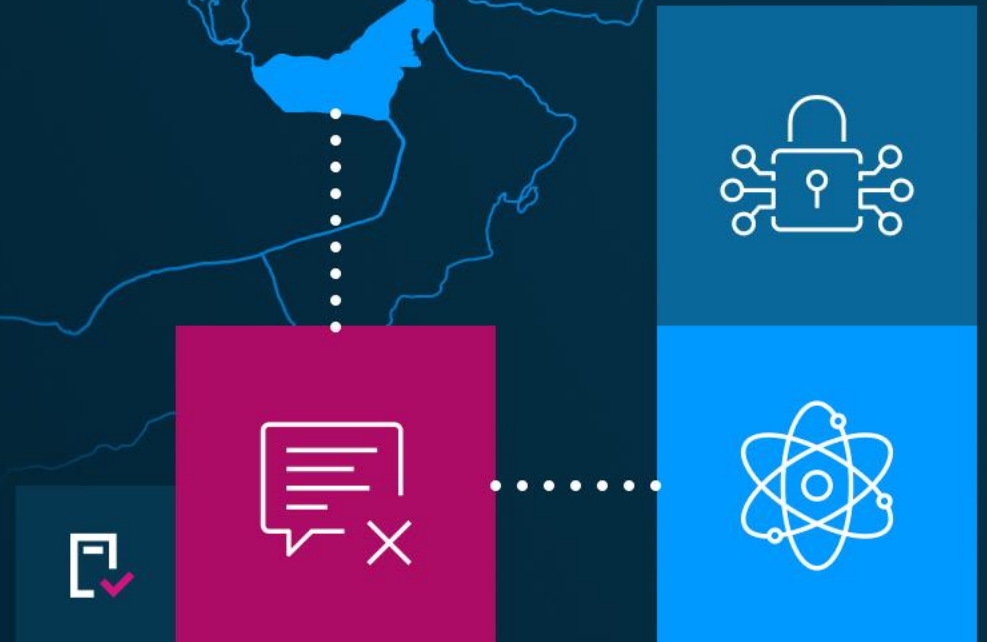




Beyond SMS OTP:

# MEETING BSP'S REQUIREMENTS WITH QUANTUM-SAFE SECURITY



# TODAY'S PRESENTERS



**ONDREJ KUPKA**

Senior Authentication  
Advisor



**BORIS FILCAK**

Partner Channel  
Manager



**MARIO DUDAS**

Technical Consultant

# ABOUT WULTRA

Wultra provides modern, post-quantum authentication designed for banks and fintech companies, ensuring secure, seamless access to digital services.

FOUNDED

2014

CUSTOMERS

70+

COUNTRIES

22

TEAM

50+



# WHAT WILL WE TALK ABOUT?

- **AFSA Circular 1213: The Shift Towards Modern Authentication**
- **Strong Authentication**
  - **Why SMS OTP Is Failing**
  - **Modern Authentication Approaches**
  - **Beyond regulatory requirements**
- **Going Beyond: Quantum-Safe and Password-less Future**
- **What to Look for in a Secure Mobile Authentication Platform**
- **Summary, Q&A**

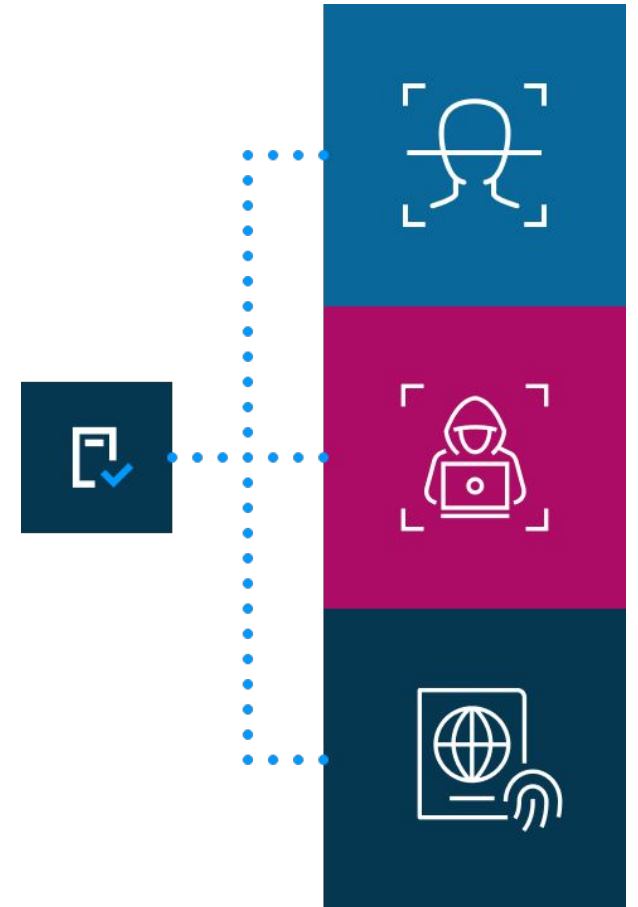
01

# AFASA CIRCULAR 1213



# REASONS FOR THE NEW REGULATION

- Consumer trust in digital channels is at risk.
- There are rising fraud cases in the Philippines, nearly **150% higher** than the world average <sup>1</sup>
- **74 %** of Filipinos reported being targeted by fraudsters, and **34 %** reported losing money due to fraud.<sup>1</sup>
- Global alignment:
  - PSD2 (EU),
  - MAS (Singapore),
  - Directive 2345 (Vietnam),
  - CBUAE (UAE)



<sup>1</sup> TransUnion: Philippines Suspected Digital Fraud Rate Higher Than Global Level for Fifth Consecutive Year

# THE MAIN TOPICS

**Strong Authentication**

**Fraud Management System**

**Customers Protection**

**Broader Responsibilities**

# THE MAIN TOPICS

**Strong Authentication**

**Fraud Management System**

**Customers Protection**

**Broader Responsibilities**

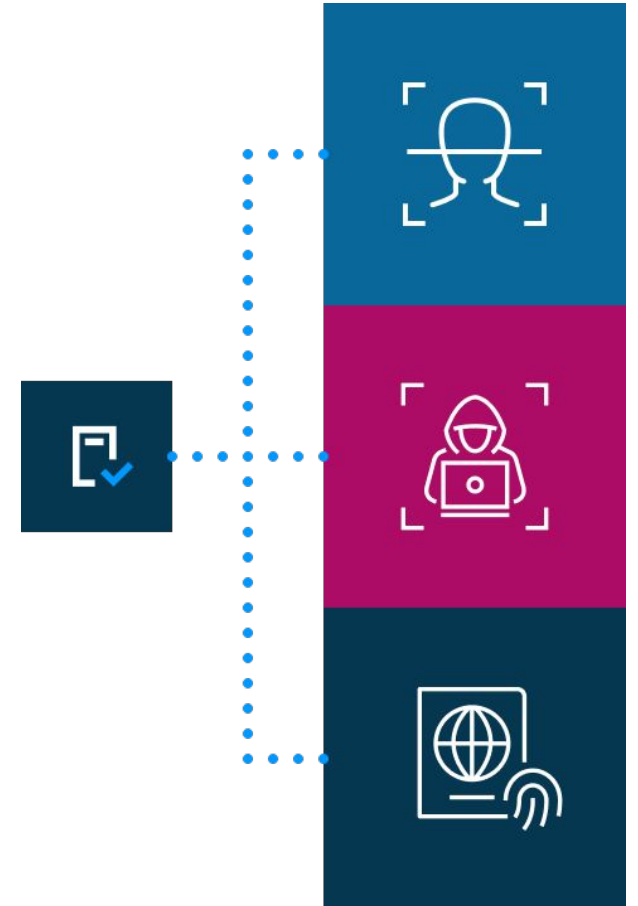
02

# STRONG AUTHENTICATION



# KEY REQUIREMENTS

- Limit SMS OTP / email OTP
- Device fingerprinting
- Real-time customer notification via secure channel
- Transaction integrity checks
- Transaction audit logs
- Strong Multi-Factor Authentication:
  - Biometrics
  - Behavioral biometrics
  - Passwordless (e.g. FIDO2, hardware keys, cryptographic binding)
  - Adaptive authentication

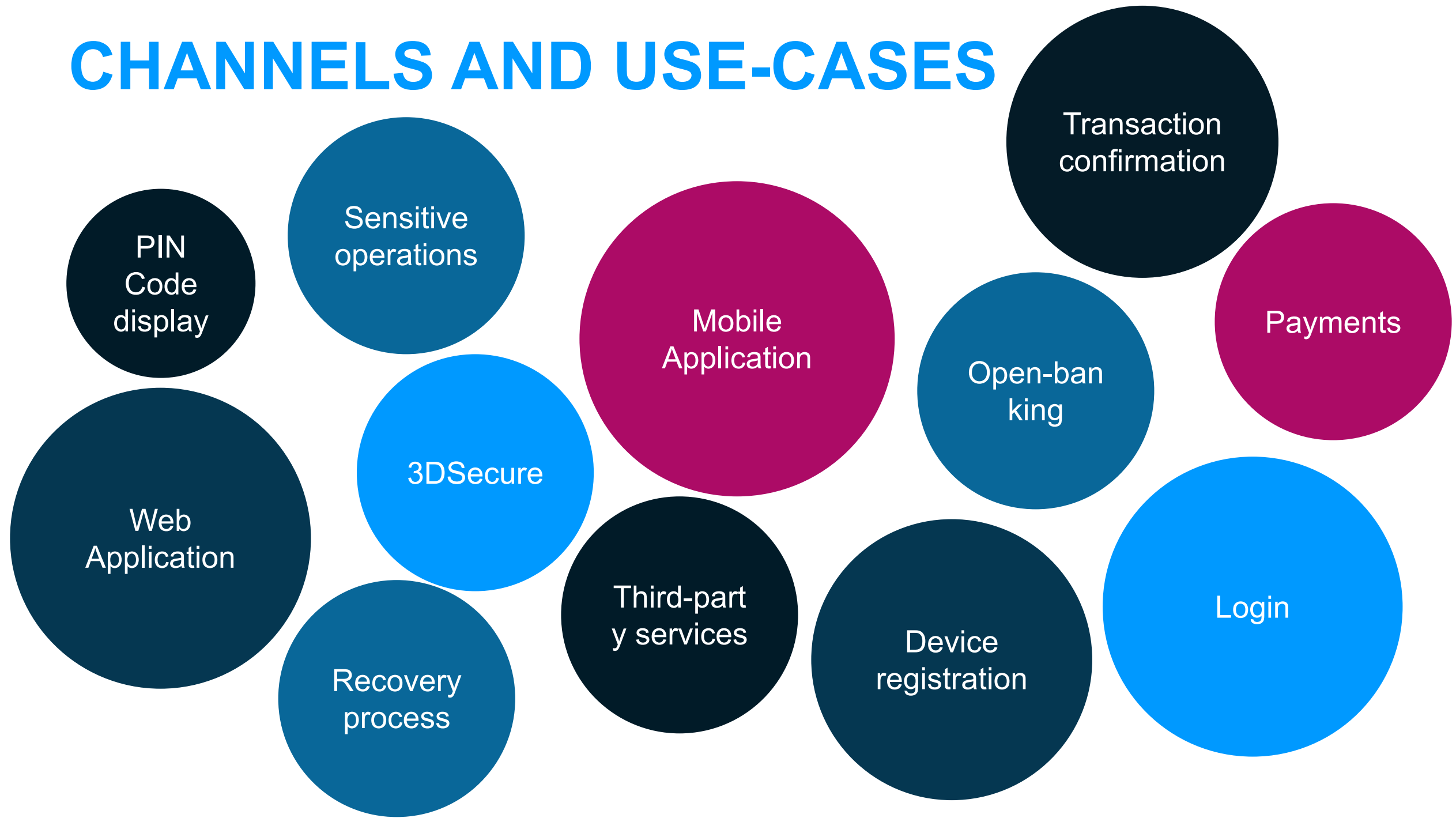


# REPLACE SMS OTP

- Easily intercepted
- Shareable credentials
- Delivery issues
- Weak user experience
- Universal attack vector



# CHANNELS AND USE-CASES



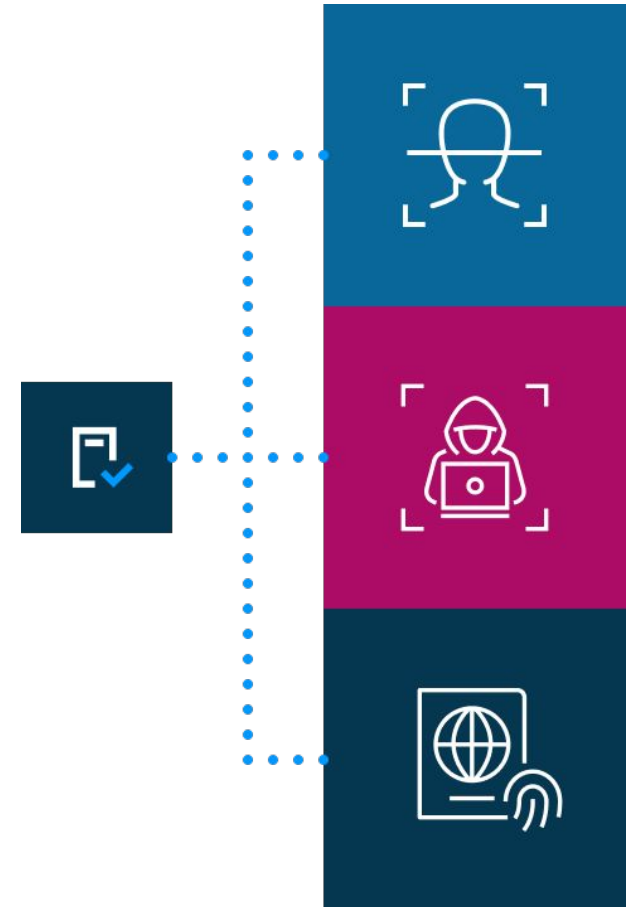
03

# PASSWORDLESS AUTHENTICATION



# PASSWORDLESS AUTHENTICATION

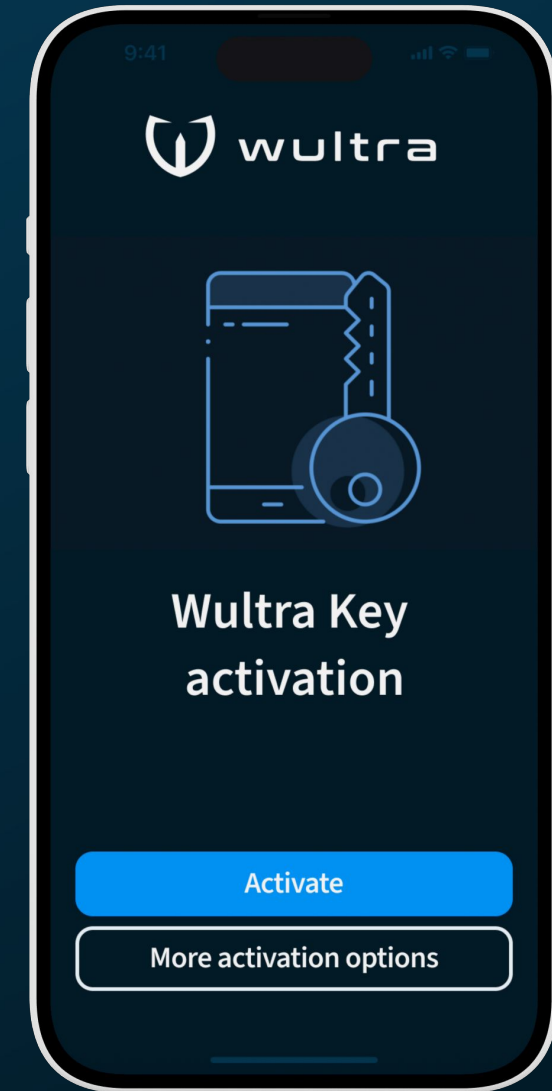
- Uses cryptographic keys, passkeys, or FIDO2 hardware tokens.
- Cryptographic keys are stored securely on the device — cannot be intercepted.
- Works seamlessly with biometrics (on-device or server-side)
- Requires device registration



# CRYPTOGRAPHIC DEVICE BINDING

- Activation with existing credentials
- Activation via web app
- Identity verification
- Branch

Note: Recovery process



**DEVICE  
FINGERPRINTING**

**X**

**CRYPTOGRAPHIC  
DEVICE BINDING**

# DEVICE FINGERPRINTING

- Collects device attributes
- Can be spoofed or cloned
- Fingerprint may change
- Invisible for user

# CRYPTOGRAPHIC DEVICE BINDING

- Generates cryptographic keys on device
- Nearly impossible to clone
- Stable and consistent identity
- Requires device registration

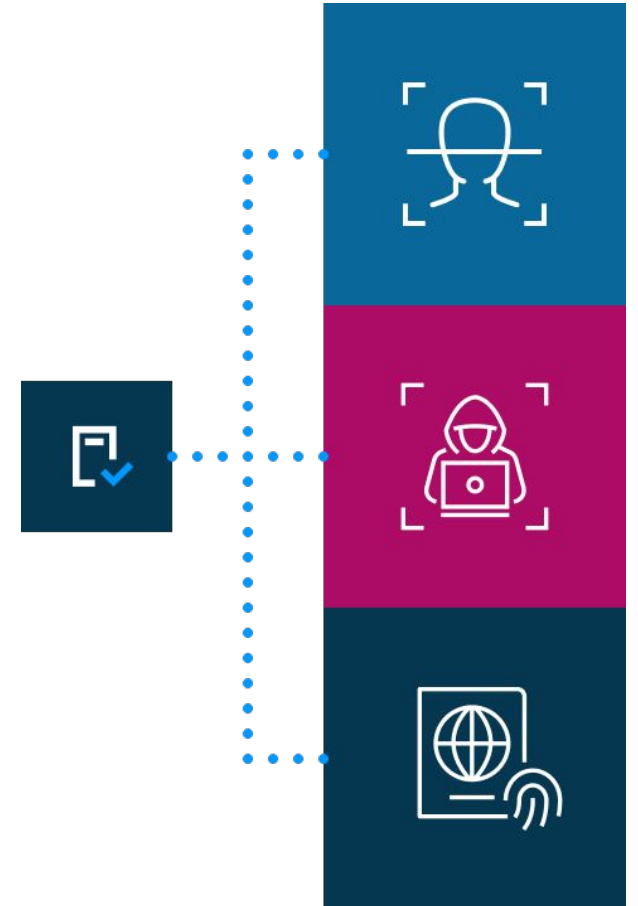
04

# BIOMETRIC AUTHENTICATION



# BIOMETRIC AUTHENTICATION

- Fingerprint, face, and voice recognition.
- Convenient, familiar to customers.
- Identity verification for various use cases:
  - Digital onboarding
  - Device registration or reactivation (recovery process)
  - Step-up Authentication



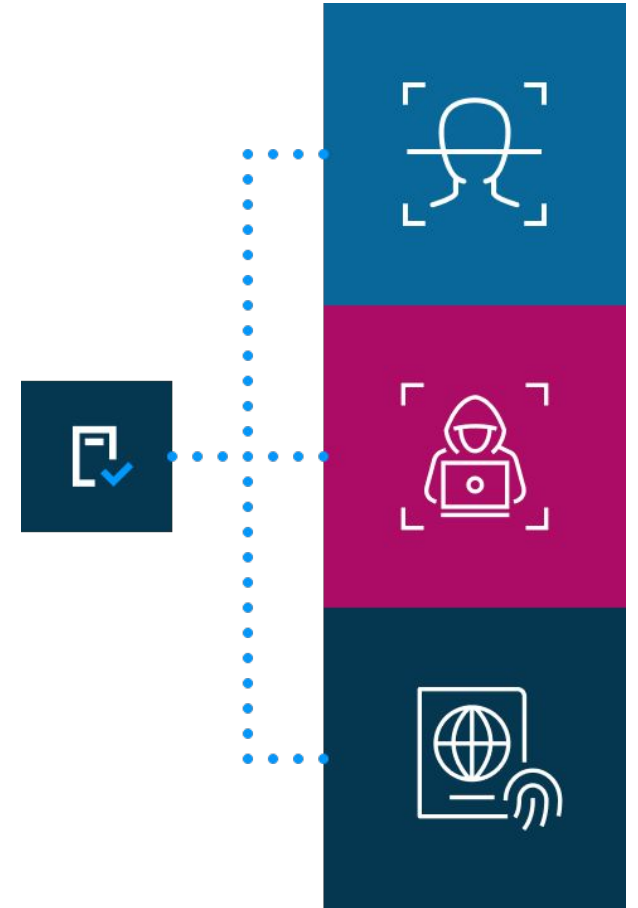
05

# BEHAVIORAL AUTHENTICATION



# BEHAVIORAL AUTHENTICATION

- Verifies how a user interacts: typing speed, swipe gestures, device tilt.
- Works in the background, no extra step for customers.
- Detects anomalies = useful for account takeover prevention.
- Best when integrated with fraud detection (continuous authentication).



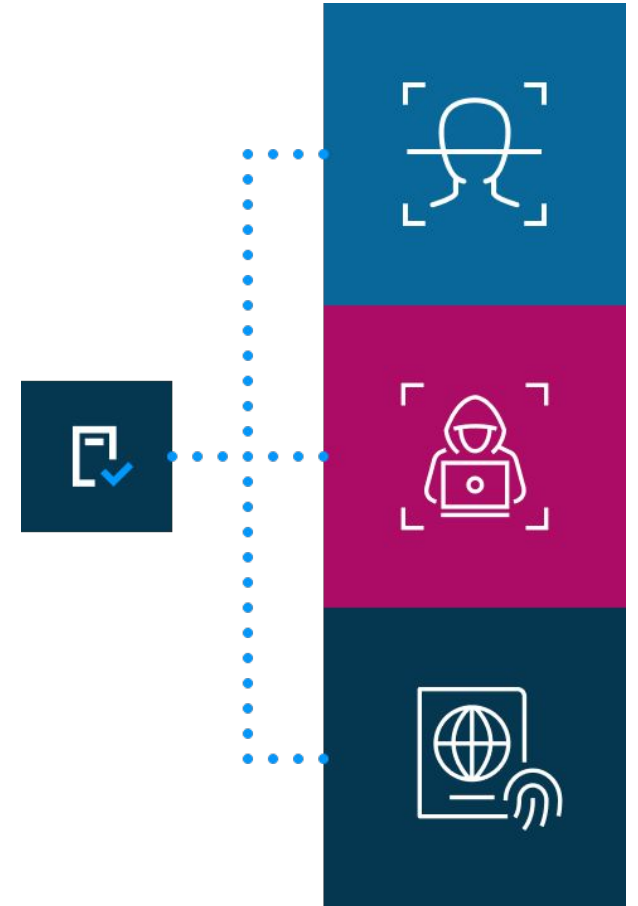
06

# ADAPTIVE AUTHENTICATION



# ADAPTIVE AUTHENTICATION

- Dynamically adjusts based on:
  - Location
  - Device
  - Behavior
  - Transaction risk
- Low risk → smooth login.
- High risk → step-up with biometrics or challenge.
- **Balances UX + security + costs.**

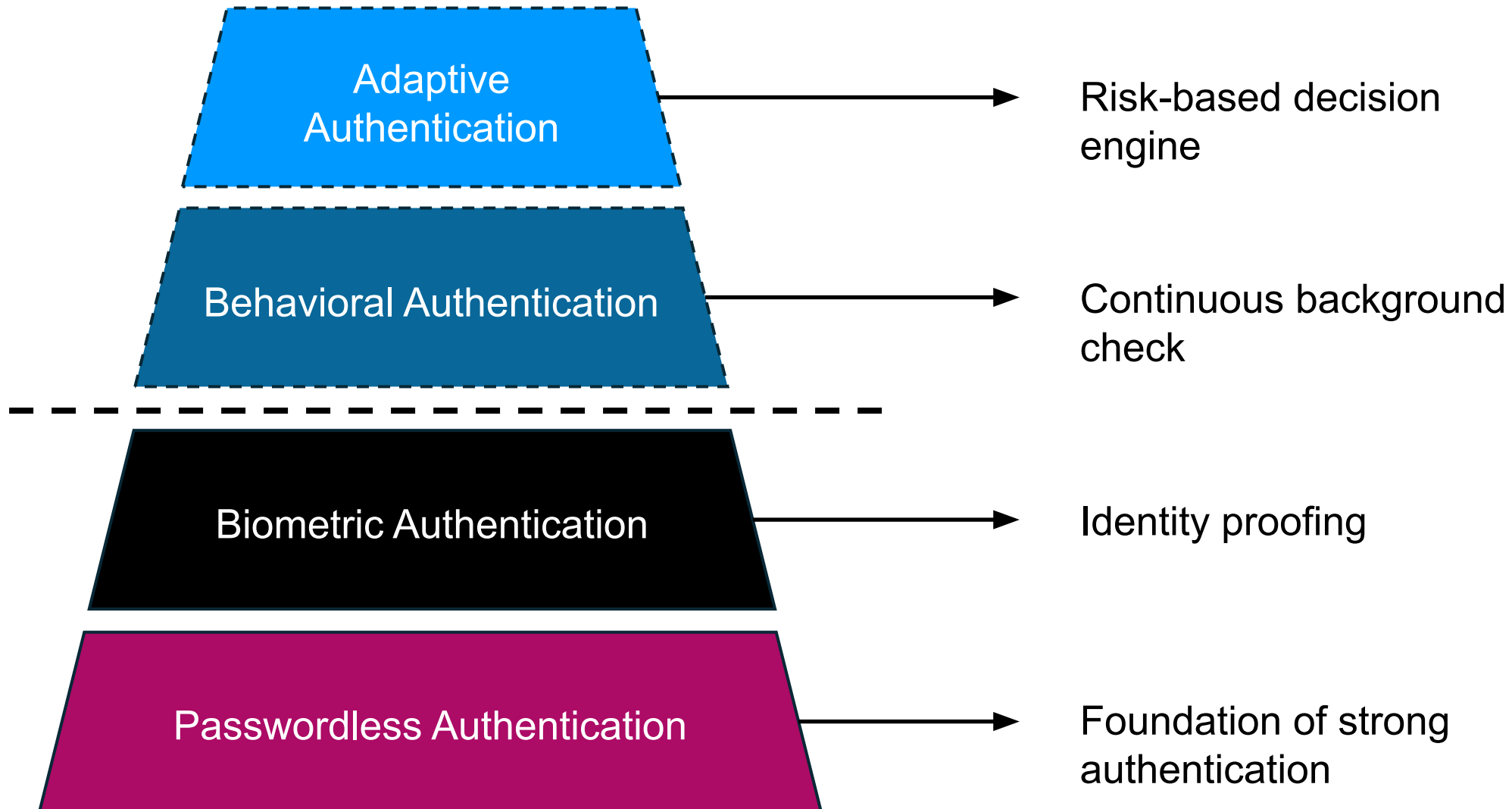


07

# AUTHENTICATION SUMMARY

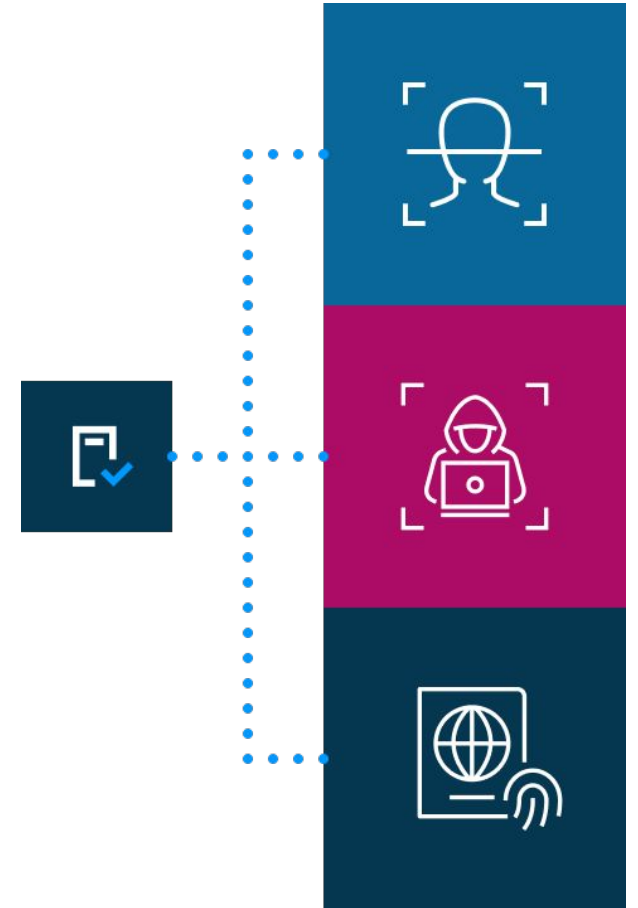


# LAYERED STRONG AUTHENTICATION



# COMPLIANT STRATEGY

- ✓ Limit SMS OTP / email OTP
- ✓ Device fingerprinting
- ✓ Strong Multi-Factor Authentication
- ✓ Real-time customer notification via secure channel
- ✓ Transaction integrity checks
- ✓ Transaction audit logs



# AUTHENTICATION FUTURE-PROOFING



**Support modern authentication standards.**



**Biometrics with advanced liveness detection.**



**Readiness for post-quantum cryptography.**



# GOING BEYOND — QUANTUM-SAFE AND PASSWORD-LESS FUTURE



WHY QUANTUM RESISTANCE MATTERS NOW?

# Growing Danger of Quantum Threat

- Quantum computing is accelerating
- Traditional cryptography won't survive the shift
- Authentication, digital signatures, and secure transactions are at risk
- Regulators are acting



Post-quantum cryptography is among the **2025 Top 10 Strategic Technology Trends**



**Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.**

By Mark Horvath, September 30,  
2024

## REGULATORY RECOMMENDATIONS

# ORGANIZATIONS SHOULD MIGRATE BY 2030



### 2025 - Start now - budget!

Education your organization on the topic of PQC, accept the fact the change is coming, and commit to the next steps.

### 2027 – RFP and Project

**Setup** approach to PQC, prepare and conduct RFPs to select solutions, contract the vendors.

### 2029 – Deprecate Legacy

Deprecate legacy solutions, only use quantum-resistant solutions.

Latest possible time to make the transition in time.

### 2026 – RFI and Market Review

Assess the impact of Q-Day by creating inventory of cryptographic metadata, inquire about information from the market vendors by conducting RFIs.

### 2028 – Projects and Migration

Implement the new solutions and migrate users from legacy solutions that use conventional cryptography to PQC.

**Wultra** is mentioned  
as the **only vendor to be  
recognized  
as a Sample Vendor** in the  
post-quantum authentication  
category.



## Request the report

Gartner, Hype Cycle for Digital Identity,  
2025, published on 14 July 2025, By  
Nayara Sangiorgio, Nathan Harris.

# HYPE CYCLE FOR DIGITAL IDENTITY 2025

**Post-quantum authentication** mentioned for the first  
time on the Gartner® Hype Cycle™  
for Digital Identity, 2025.

# MOBILE-FIRST AUTHENTICATION

Using a mobile app to log in and sign transactions in any digital channel.

## MULTI-FACTOR AUTHENTICATION

### 1ST FACTOR



#### POSSESSION

Registered mobile device (device binding)

### 2ND FACTOR



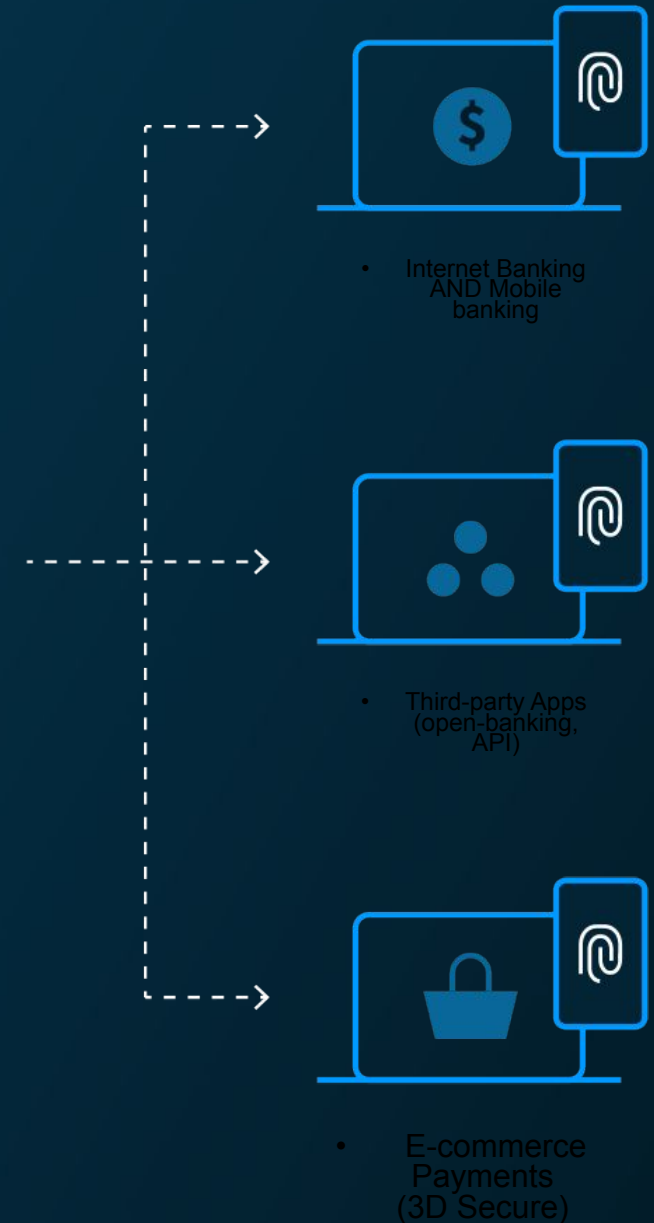
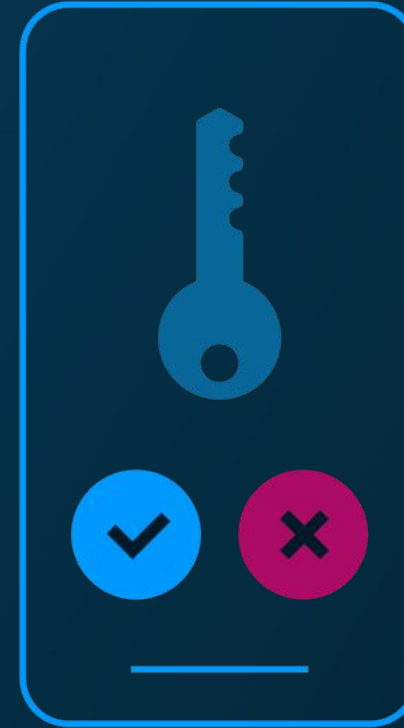
#### KNOWLEDGE

PIN code or password



#### INHERENCE

Device biometrics (Face ID, Touch ID)



## POST-QUANTUM AUTHENTICATION

# THE SAME UX, SUPERIOR SECURITY

We must switch to quantum-resistant cryptography so we can continue using the online services we love.

### HYBRID SCHEME



#### ECC + CRYSTALS

Trusted classical algorithms + future-proof PQC.

### CRYSTALS



#### ML-KEM (KYBER)

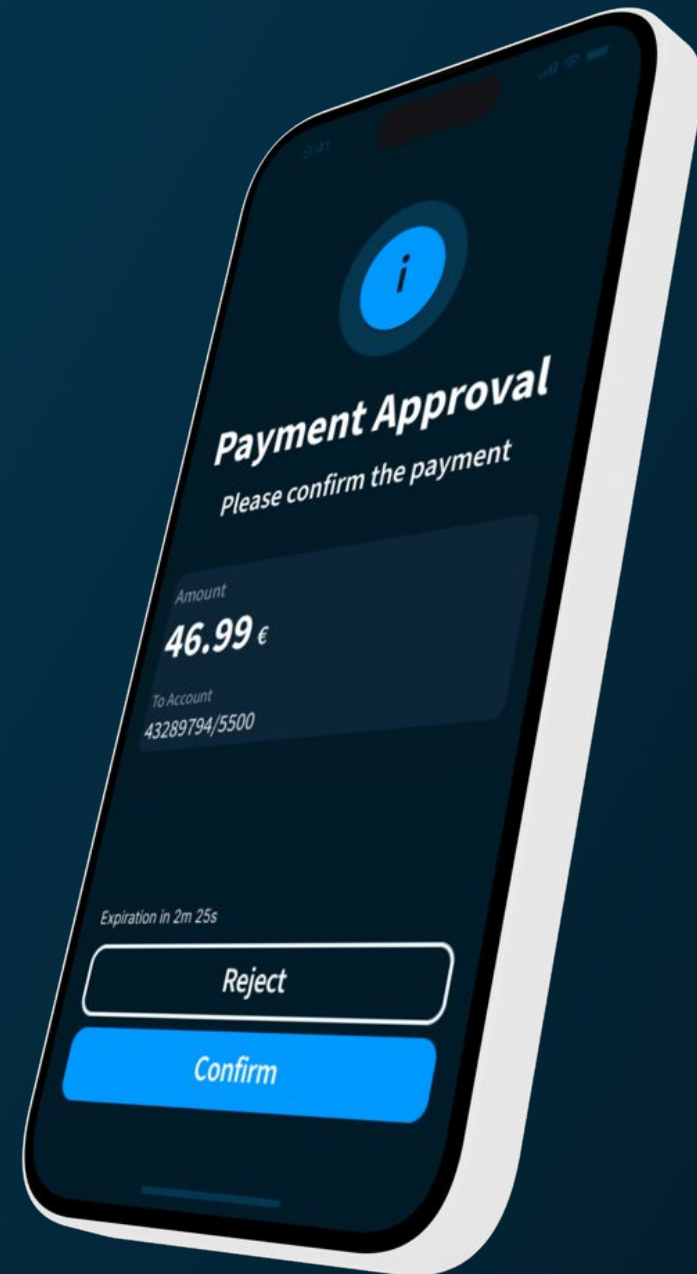
KEM, establishes key for AES-256.



#### ML-DSA (DILITHIUM)

Digital signatures.

**NIST**  
National Institute of  
Standards and Technology



# POST-QUANTUM AUTHENTICATION PLATFORM

## 1. MOBILE-FIRST AUTHENTICATION

### Mobile Token Standalone App



### Mobile SDK Plugin for Your App



### Talisman FIDO2 Hard Token



### Post-Quantum Passkeys Built-in Authentication



**POWERAUTH INFRASTRUCTURE**  
Deployed On-Premise or in the cloud

# SECURED BY IN-APP PROTECTION

Protect the authentication process  
on insecure hardware.



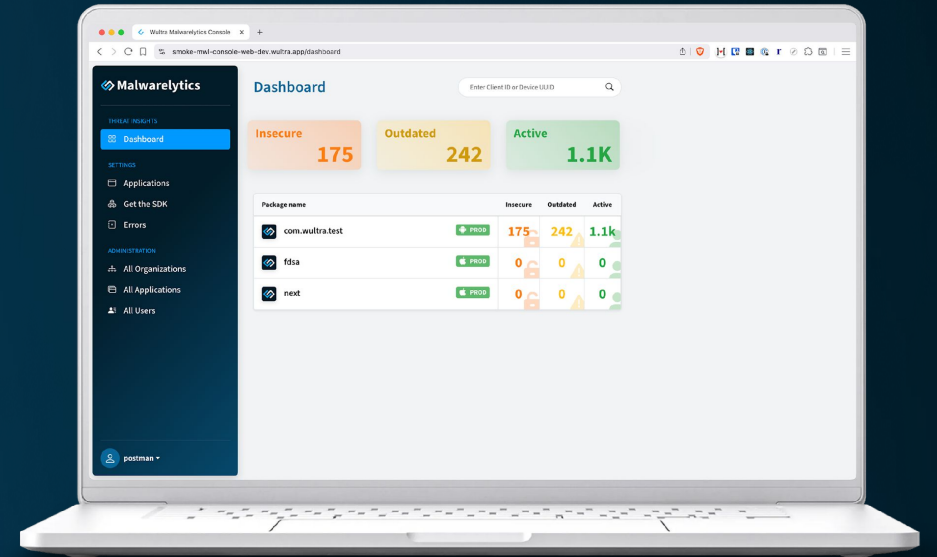
**PROTECTS THE RUNTIME  
OF THE APPLICATION**



**DETECTS POTENTIAL THREATS  
ON THE MOBILE DEVICE**

Warn or block users straight away.  
Feed the data to fraud detection systems.

**10 MINUTES  
TO INTEGRATE**



# SUPPORTED FEATURES

Our security suite allows CISOs to comply with the strictest OWASP standard requirements on mobile app security and mobile application resilience.

## COMPONENTS



### ANTI-MALWARE

- ✓ Malware threat identification
- ✓ Malware threat mitigation
- ✓ Listening to app changes
- ✓ Installer identification
- ✓ Smart protection
- ✓ Smart protection UI customization

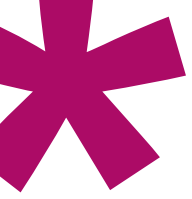


### RASP (Runtime Application Self-Protection)

- ✓ Detection of attached debuggers
- ✓ Detection of emulators
- ✓ Detection of rooted devices
- ✓ Detection of app repackaging
- ✓ Blocking screen readers
- ✓ Detection of screen sharing/screen mirroring
- ✓ Blocking screenshots of app screens
- ✓ Tapjacking protection
- ✓ Detection of HTTP proxy
- ✓ Detection of VPN
- ✓ Detection of usage of system screen lock
- ✓ Obtaining Play Protect status
- ✓ Changing app process name
- ✓ Detection of ADB status
- ✓ Detection of developer options status
- ✓ Detection of biometry enrollment status
- ✓ Detection of active call
- ✓ Detection of application presence
- ✓ Activity protection
- ✓ RASP observer



[EXPLORE  
DOCUMENTATION](#)



# OTHER MOBILE THREATS YOU NEED TO ADDRESS



REMOTE DESKTOP  
APPLICATIONS



SCREEN SHARING &  
UNTRUSTED SCREEN  
READERS



SCREENSHOTS OF  
SENSITIVE DATA



VOICE-BASED  
SCAMS

## How to mitigate:

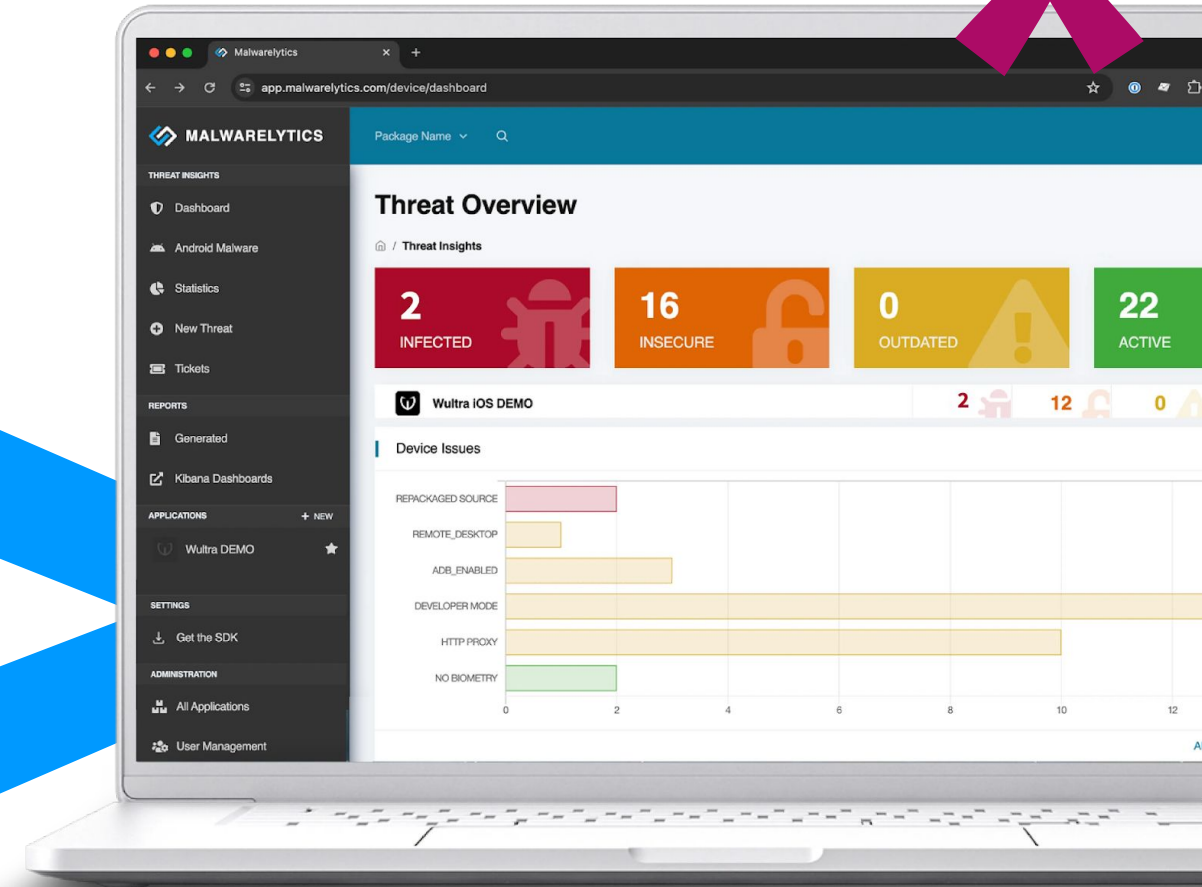
- Strengthen authentication (no SMS OTPs)
- Fortify your apps with **in-app protection**
- Detect and respond to real-time risks in the mobile environment



# WEB CONSOLE

Easily accessible web interface, that allows you to:

- Monitor current threats
- See the important trends
- Examine device details and events
- See the present malware on devices
- See installation sources
- Monitor device statistics
- Examine device attributes (jailbreak/rooting, remote desktop, developer mode, outdated OS, etc.)



06

# SUMMARY, Q&A



# THANK YOU!

