KEYPASCO PLATFORM

Attackers Don't Hack Your System. They Log In with Your Users' Passwords.

Stop account takeover before it destroys your business.

122%
YoY surge in fintech ATO attacks

26B
Credential stuffing attempts/month

EBA has restricted SMS OTP scope. The EU's new PSR is expected to phase it out entirely.
Is your platform ready?

› KEYPASCO PLATFORM — EMBED MFA INTO ANY APPLICATION

★ API-first Integration

Flexible API that embeds into any platform and adapts to your existing stack.

★ Stops ATO & Fake Accounts

Two-channel + Device Fingerprints block credential stuffing, account takeover and bot registrations.

★ Built for Compliance

Privacy by Design minimal data retention, end-to-end encryption. Covers PSD2 SCA, GDPR, ISO 27001, and FIDO2.

★ Supports FIDO2

Passwordless, phishing-resistant, hardware-attested authentication.

› CORE FRAUD PREVENTION TECHNOLOGY

Two-channel Structure

Even if passwords are stolen or OTPs intercepted, fraudsters still cannot log

Auth requests and responses travel on completely independent channels, eliminating man-in-the-middle attacks at the root. Addresses CRA Annex I 3(b) unauthorised access prevention.

Device Fingerprints

Your account can only be accessed from your device. Unknown devices are blocked, no exceptions.

Every login is bound to a known device profile. Unregistered devices are auto-blocked regardless of credential validity. Aligns with CRA Annex I secure-by-default principle.

Additional MFA Mechanisms

Split PKI Sign | Proximity | Geo-time Control | Risk Management Engine

› SUPPORTS FIDO2 AUTHENTICATION

Password-less

Private keys never leave the device, no credentials transmitted, nothing to intercept, steal, or phish.

Origin Binding

Bound to the legitimate origin. Fake sites can't intercept or replay.

Key & Device Attestation

Cryptographic proof the key and device are genuine and uncompromised

› REAL THREATS. REAL ANSWERS

Fintech / Digital Banking

SMS intercepted, account drained in minutes: **Independent channel makes interception useless**	**Two-channel Structure**
Leaked credentials used to take over accounts: **Device binding means stolen passwords can't log in**	**Device Fingerprints**
Server breached and credentials stolen in bulk: **Stolen server fragment is worthless without the device and biometric**	**Split PKI Sign**

E-commerce / Subscription Platforms

Bots mass-register fake accounts to exploit promotions: **Device fingerprint exposes bulk registration instantly**	**Device Fingerprints**
Bots remotely complete high-risk transactions: **Physical proximity requirement renders remote bots ineffective**	**Proximity**
Account accessed from unusual location to place fraudulent orders: **Geo-time controls flag and block anomalies instantly**	**Geo-time control**

Your platform is ready. Is your authentication?

Get in touch. keypasco.com | sales.eu@keypasco.com