

KEYLESS

Biometric Authentication Without Storing Biometric Data

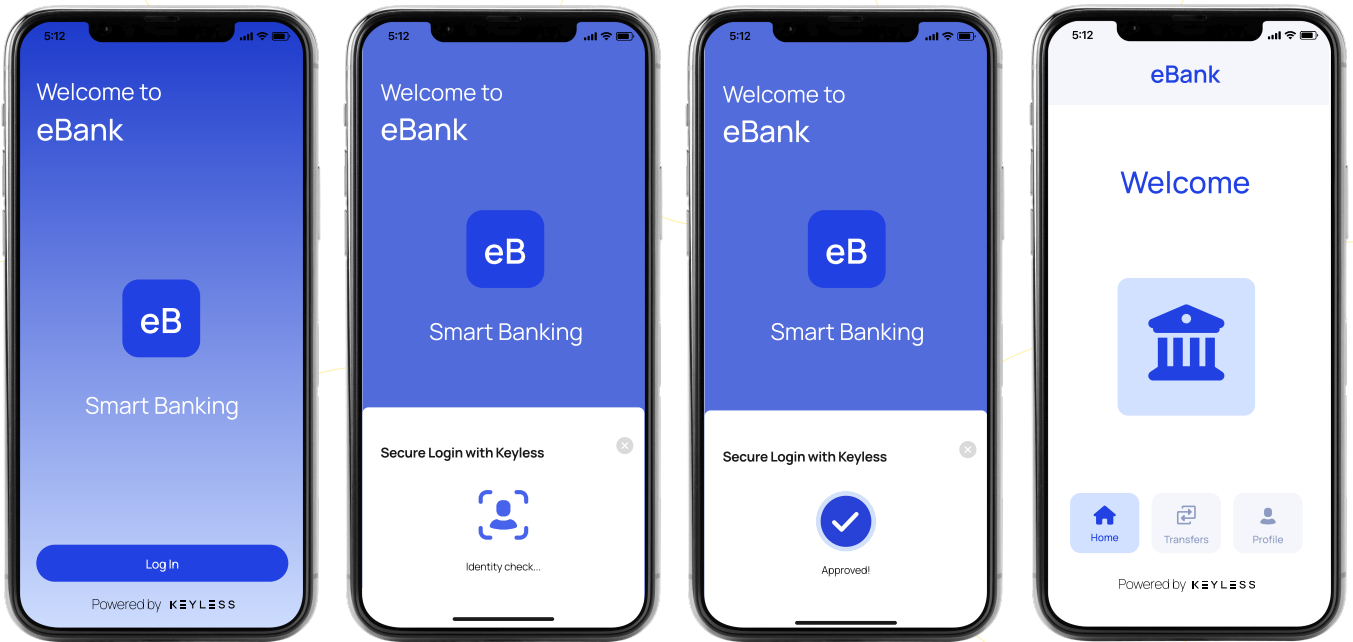
Privacy-preserving biometric multi-factor authentication for your customers and workforce with one glance.

TRUSTED BY LEADING ORGANIZATIONS

INTESA SAMPLOLO moneyfarm Q8 LUISS experian prometeia

ASSESSED AND FEATURED BY

Gartner Liminal kuppingercoale ANALYTICS fido ALLIANCE fime CB INSIGHTS



Strong Customer Authentication with in-built MFA

True multi-factor authentication - device and face - with one glance.

Guaranteed Biometric Privacy

No biometric data stored anywhere - neither on device or cloud.

Genuine Identity Assurance

Authenticate the person who enrolled their account, not their device.

Reduce Account Recovery Costs

Reduce reliance on customer help desk and SMS OTP costs.

Silent Enrollment

Passive backend enrollment of existing users into Keyless using IDV provider images.

KEYLESS

info@keyless.io

www.keyless.io

KEYLESS FOR CUSTOMERS



Enrollment: Close the gap between identity verification and biometric authentication with the Keyless IDV Bridge. Rapidly enroll users onboarded via IDV and KYC using existing images, requiring no action from them.



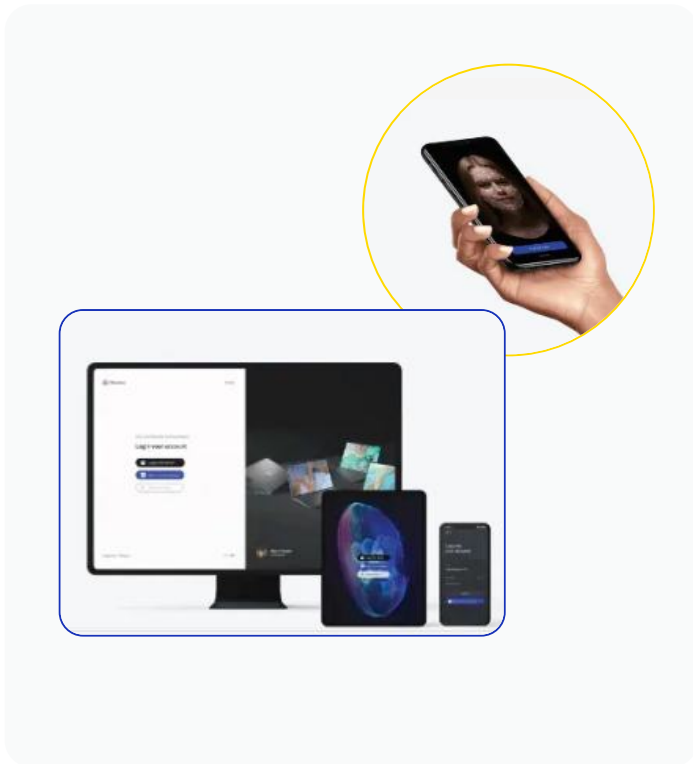
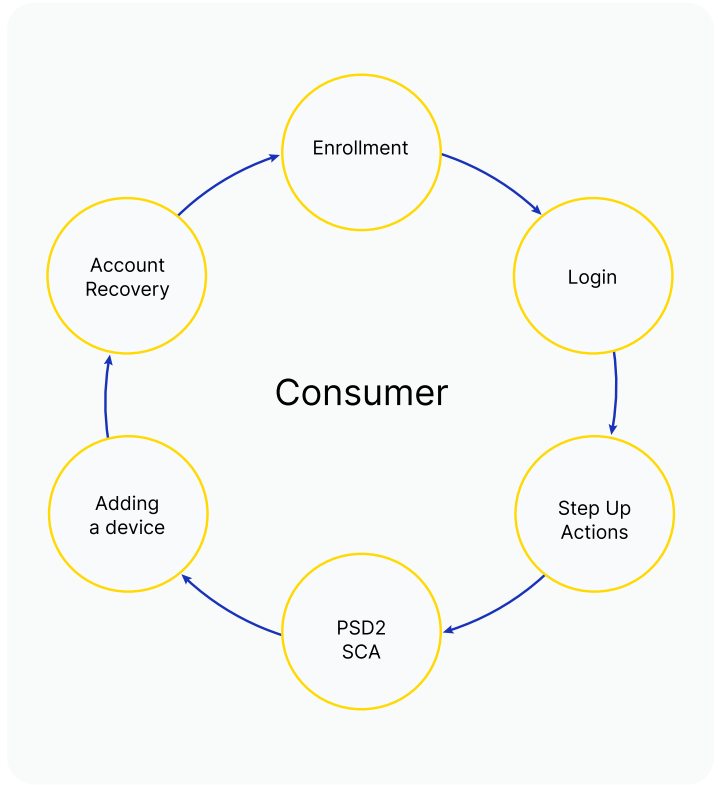
PSD2 SCA Compliance: Built for banks, Keyless is multi-factor by design and provides dynamic linking for all electronic transactions with a simple selfie.



Login and Step-Up Authentication: Secure logins and higher-risk user actions from ATO fraud by replacing or complementing OTPs with biometric authentication.



Self-Service Account Recovery: Slash call center and SMS OTP authentication costs with a self-service account recovery selfie that matches their biometric profile with the data created during account registration.



KEYLESS FOR WORKFORCE



Passwordless SSO: Securely authenticate employees accessing identity management systems by replacing passwords with a biometric selfie.



Employee MFA: Implement with your preferred identity provider or application, whether through the Keyless Authenticator or integrated into your existing app.



Shared Devices: Enable employee authentication on any shared device with a front-facing 720p camera. Reduce administration costs associated with credential management, resets, and lost tokens.



VPN & VDI: Unify all your remote logins and improve workforce security with VPN and VDI integrations.

