DATASHEET

Entrust Biometric Passkey

Stop Impersonation. Eliminate Friction. Prove It's Really Them.

Overview

Entrust Biometric Passkey is an identity-bound, phishing-resistant authentication solution that combines the security of cryptographic passkeys with the assurance of verified biometrics. Unlike standard passkeys that prove device possession, our passkey solution proves the right verified person is present – not just the right device.

Designed for financial institutions, fintechs, and digital platforms – the solution works like any passkey for everyday logins. Users offer a glance or a fingerprint, nothing more. When risk is elevated, security steps up automatically, matching the user's live biometric against their verified identity. Same product, different modes. Users never have to manage the difference.

The biometric passkey integrates with existing IAM through REST APIs, SDKs, and WebAuthn/CTAP with no rip-and-replace required. The result: a seamless, enterprise-grade authentication layer that converts faster, retains more customers, and closes the gaps attackers exploit most.

Benefits

Entrust Biometric Passkey delivers measurable impact across security, user experience, and business outcomes.

Frictionless Everyday Authentication: Customers log in with a glance or a fingerprint. No passwords, no OTPs, no interruptions. The passkey handles low-risk authentication invisibly, so users move through their day without noticing the security behind it.

High-Assurance When It Counts: For risky moments like wire transfers, device enrollment, account recovery, etc., Biometric Passkey triggers a real-time biometric match against a previously verified identity. Precision friction, only when warranted.

BENEFITS

1. No passwords. No OTPs. No friction.
2. Verified identity, not just a device
3. Self-service recovery, zero agent risk
4. One identity across the full lifecycle

KEY FEATURES

- Recover accounts without interrupting the customer experience
- High-risk moments feel safe and trusted
- Reduced risk of negative reputation and customer turnover rates

ENTRUST
SECURING A WORLD IN MOTION

Why Standard Passkeys Are Not Enough

Standard passkeys are a meaningful step forward, eliminating passwords while resisting phishing attempts. But they carry critical limitations. They prove that a device is present, but not a person. This creates real exposure in the moments that matter most:

- Stolen or shared devices can still authenticate successfully. The passkey has no way to confirm who is actually holding the phone.
- Enrollment and recovery flows remain open to impersonation. An attacker who takes over an account can add a fraudulent passkey tied to a new device.
- Cloud-synced passkeys move across devices without re-verifying the person, creating invisible risk when credentials migrate to a new handset.
- Standard passkeys do not satisfy strong customer authentication requirements where regulators expect a verified biometric, not just a device PIN or Face ID.

The Entrust Difference: Identity-Bound Authentication

Standard passkeys prove a device is present. Entrust Biometric Passkey proves a verified person is present. This distinction matters when devices are stolen, shared, or socially engineered. Every passkey is bound to a verified human identity, matched against a trusted record established at onboarding. Key differences include:

- Device-bound, not cloud-synced: The passkey stays on the device it was issued to, reducing exposure from credential migration
- Identity-verified enrollment: New passkey is issued only after confirming the request comes from the legitimate account holder
- Biometric verification at step-up: Risky actions trigger a real-time biometric comparison against the Encrypted Biometric Token (EBT) stored at enrollment
- One verified identity, reused across the lifecycle: No re-enrollment at recovery, no additional friction for returning customers

Built for Financial Services

Entrust Biometric Passkey was designed for the regulatory and operational reality of financial institutions. It is built to meet strong customer authentication requirements, satisfy audit and compliance demands, and operate within the data sovereignty constraints of regulated environments.

- The Biometric Passkey server is self-hosted within the bank's infrastructure. The bank is the data controller for credential metadata and biometric tokens.
- Entrust Workflow Studio acts as the data processor for IDV and biometric comparison during high-risk events, with clear data processing boundaries.
- Our solution is built with React Native and Flutter SDK support for rapid integration into existing mobile banking applications.

HOW IT WORKS

Every Moment. One Continuous Identity.

Entrust Biometric Passkey operates across the full customer lifecycle, adapting the level of assurance to the risk of the moment:

Step 1: Identity Verified Enrollment

When a customer registers a passkey on a new device or for the first time, Entrust verifies their identity against a government-issued document and biometric check. Device biometrics alone are not accepted. The passkey is issued only after the person is confirmed.

Step 2: Frictionless Everyday Login

For routine logins, the customer uses native device biometrics (Face ID, Touch ID, fingerprint) or a PIN to unlock the passkey. No biometric comparison to the EBT is triggered. The experience is identical to a standard passkey. Fast, effortless, and invisible.

Step 3: Risk-Triggered Step-Up

When a risk engine flags elevated risk, the system prompts a face authentication or motion authentication check. The live capture is matched against the stored EBT in real time. Only a confirmed match proceeds.

KEY FEATURES & BENEFITS

Risk-Adaptive Authentication

Entrust Biometric Passkey does not apply the same level of friction to every interaction. Standard logins use native device biometrics through the passkey flow, fast and invisible. High-risk moments trigger a biometric comparison against the verified EBT, adding assurance precisely when needed. The result is a system that feels effortless to legitimate customers while presenting a meaningful barrier to attackers. This adaptive model ensures that authentication friction is proportional to risk and not applied uniformly in a way that degrades experience for the majority to protect against the minority.

Phishing-Resistant Cryptographic Credentials

Passkeys use asymmetric cryptography: the private key lives on the device, the public key is stored server-side. There is no shared secret to phish, no OTP to intercept, no password to steal. Combined with Entrust's identity binding, the result is a credential that is both phishing-resistant and impersonation-resistant. For financial institutions facing increasingly sophisticated phishing and social engineering campaigns, this combination closes two distinct attack vectors with a single authentication flow.

Deepfake-Resistant Liveness Detection

Entrust's biometric engine includes advanced liveness detection built to resist AI-generated face attacks, pre-recorded video replays, and camera injection exploits.

As deepfake technology becomes more accessible to attackers, passive liveness alone is no longer sufficient. A biometric check is used at step-up and high-risk moments to confirm a live, physically present person. The biometric engine is continuously updated against emerging attack vectors and synthetic images.

Self-Service Account Recovery

Account recovery is among the highest-risk moments in the customer lifecycle. Most recovery flows rely on SMS, email, or agent-assisted processes, all vulnerable to social engineering and SIM swap attacks. Entrust Biometric Passkey replaces these with biometric self-service recovery, matching the customer's live face against the EBT established at enrollment. This eliminates agent-assisted recovery risk, reduces support costs, and gives customers a faster, more trusted path back to their account.

IAM-Agnostic Integration

Entrust Biometric Passkey is not a replacement for your IAM. It is a verified identity layer that sits alongside your existing stack. Integration is delivered via REST API for web applications and native mobile SDKs for iOS and Android, supporting React Native and Flutter frameworks. WebAuthn and CTAP compliance ensures compatibility with modern browsers and platform authenticators, making it deployable across web and mobile channels without rebuilding existing authentication infrastructure.

Capability	Details
Authentication Methods	Passkey (FIDO2/WebAuthn) with biometric step-up and native device biometrics (Face ID, Touch ID, PIN)
Identity Binding	Passkey bound to verified identity via Encrypted Biometric Token (EBT) at enrollment
Liveness Detection	Advanced active and passive liveness; injection attack and deepfake resistant
Enrollment Flows	New EBT creation; cross-platform and mobile-native flows
Step-up Triggers	Risk engine integration; high-value transactions; new payee; suspected ATO events
Account Recovery	Biometric self-service recovery tied to verified EBT; no SMS or agent dependency
IAM Integration	Works with all major IAM and IDV providers; REST API
Mobile SDKs	iOS and Android native; React Native; Flutter
Web Support	WebAuthn / CTAP; QR code cross-platform flow for desktop-initiated high-risk events
Deployment Model	Biometric Passkey server self-hosted in bank infrastructure; Entrust Workflow Studio cloud-hosted
Data Control	Bank is data controller for EBTs and credential metadata; Entrust is data processor for IDV and biometric comparison
Compliance Alignment	Supports strong customer authentication requirements; audit log maintained on-premise

Ready to see Entrust Biometric Passkey in action?

Request a demo or speak with an identity expert at entrust.com

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION