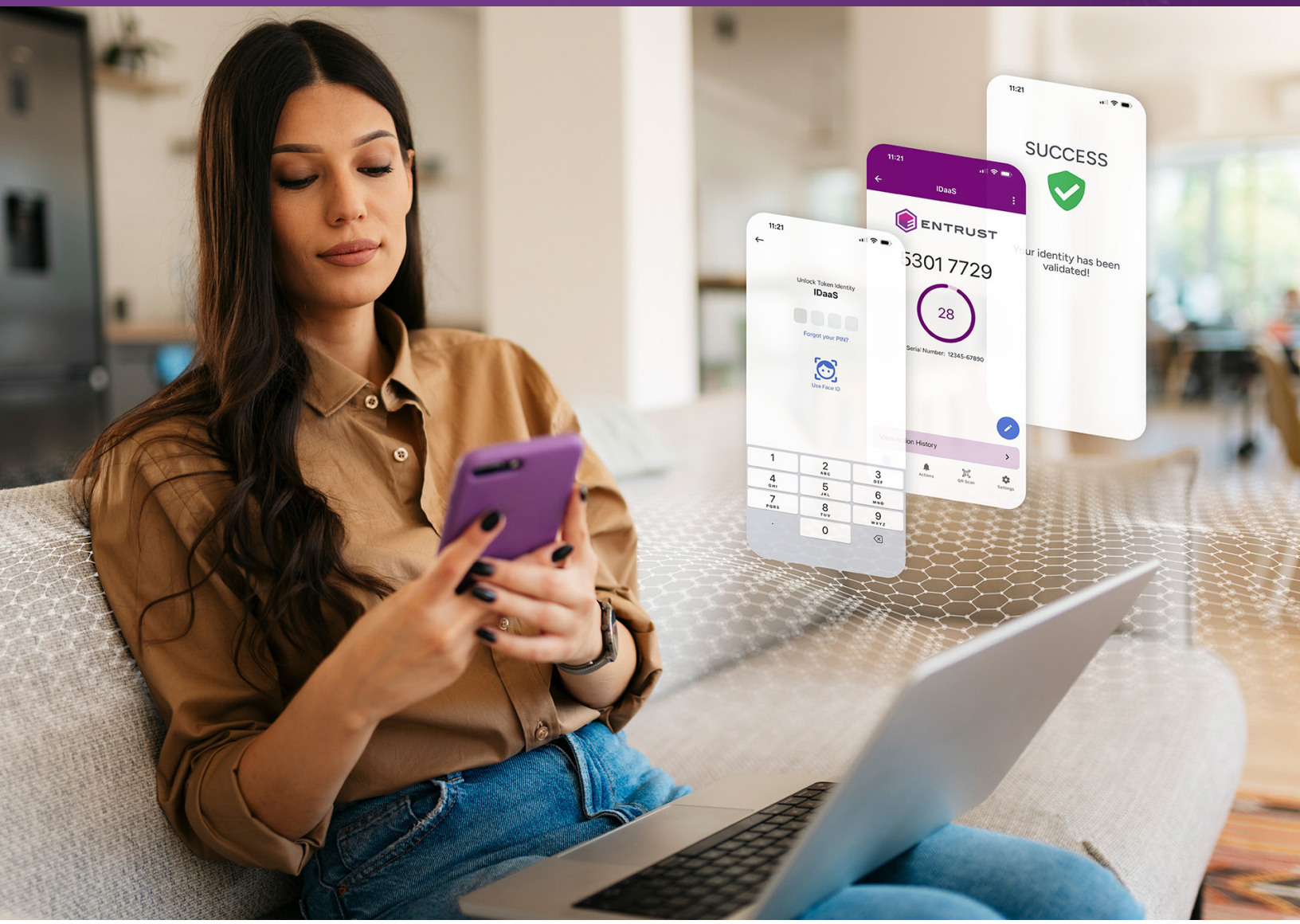
Authentication

Modern Authentication for Trusted Customer Experiences



ENTRUST

SECURING A WORLD IN MOTION

The Modern Authentication Challenge

Digital services are expanding rapidly from account opening to everyday logins, payments, and high-value transactions. Yet the threat landscape is evolving just as quickly. Credential compromise, phishing, automated attacks, and increasingly sophisticated AI-driven impersonation continue to expose the weaknesses of identity systems that were never built for continuous, high-risk engagement.

Traditional methods, such as usernames, passwords, and basic one-time passcodes, were designed for a simpler era. Today, they create friction for legitimate users while remaining vulnerable to credential stuffing, social engineering, and account takeover attempts. Security controls also tend to be inconsistent across the user journey: strong during new user onboarding, weaker at login, and largely reactive during transactions. This often results in fragmented security and unnecessary operational complexity.

When authentication fails to protect consistently, fraud exposure rises, account takeover becomes harder to detect, and recovery costs climb. But when authentication introduces too much friction, users abandon onboarding flows, delay transactions, or lose confidence in their provider. Organizations end up facing a false tradeoff between protection and usability – a tradeoff that directly impacts conversion rates, customer lifetime value, and brand trust.

A recent consumer survey conducted by Entrust underscores this tension. The report found that 35% of consumers rank biometric authentication as the most trusted method, far ahead of passwords, with two-thirds willing to use biometric authentication methods. More critically, more than half – 56% – say they would switch banks after experiencing fraud, highlighting how quickly trust can erode.

These findings show a clear shift in expectations: users increasingly see stronger authentication not as added burden, but as better experience. Modern authentication must therefore move beyond static credentials and isolated checkpoints. It must be identity-centric, risk-aware, and capable of continuously validating the right user, in the right context, at the right time, at scale and without unnecessary friction.

Entrust secures identity at global scale – recognized in both the Gartner® Magic Quadrant for Identity Verification and the Gartner® Magic Quadrant for Access Management, one of the only vendors to appear in both. Trusted by organizations that cannot afford to get identity wrong, our platform helps deliver measurable results including up to 60% reduction in customer abandonment, 50% fraud reduction, and sub-three-second biometric matching across 195+ countries.

35% of consumers rank biometric authentication as the most trusted method, far ahead of passwords – and two-thirds are willing to use it.

Modern Authentication, Unified on One Identity Platform

Modern authentication requires more than stronger login controls for many reasons. Organizations need to:

- Provide secure, trusted access to the right users at the right time
- Quickly and seamlessly revalidate users throughout high-risk interactions
- Deliver consistent experiences throughout the customer lifecycle, from onboarding to everyday authentication and high-risk moments
- Meet increasingly demanding regulatory compliance mandates

Meeting these demands requires a unified identity foundation – one that connects onboarding, access, transaction protection, and digital approvals into a seamless, continuous trust framework. Entrust delivers this through an integrated platform that brings together Identity Verification (IDV), Identity and Access Management (IAM), and digital signing. Rather than relying on siloed solutions, Entrust enables organizations to validate users from the moment they enter the ecosystem through every interaction that follows, providing consistency, continuity, and intelligence across the entire identity lifecycle.

With this unified approach, authentication is no longer an isolated event – it becomes a persistent validation process embedded across onboarding, login, and high-risk moments. The result: stronger identity assurance, reduced fraud exposure, and a better user experience, simultaneously.

Unified Identity Verification and Authentication

Entrust anchors authentication to verified identity. Using global document verification and AI-powered biometric validation – including sub-three-second matching and PAD Level 2 liveness detection – organizations establish a high-assurance identity at onboarding. That verified identity is then reused across future authentication and account recovery events, reducing impersonation risk and eliminating redundant friction for legitimate users.

Risk-Based Adaptive Authentication

To ensure the right level of assurance at the right time, Entrust continuously evaluates contextual signals such as device posture, location, and transaction risk. Low-risk interactions remain seamless, while elevated-risk events automatically trigger stronger authentication. This dynamic, Zero Trust-aligned model helps strengthen security precisely where it matters most, without degrading user experience.

Phishing-Resistant Multi-Factor Authentication (MFA)

With credential compromise still the most common attack vector, Entrust offers strong, phishing-resistant MFA that moves beyond SMS one-time codes toward biometrics, device-based trust, and mobile push verification. Entrust adds orchestration capabilities, multi-authenticator registration, and passwordless options, including Magic Link, to further improve usability and reduce abandonment across channels.

Trusted Digital Signing

Authentication must also extend into transaction approvals and digital agreements. Entrust binds signatures to verified identity and authentication events, creating tamper-evident, auditable records for high-value actions. This strengthens assurance for sensitive workflows and supports compliance in regulated environments.

Together, these capabilities operate within a single, unified architecture, so security teams reduce complexity, fraud teams gain stronger controls, digital teams deliver frictionless experiences, and compliance teams meet KYC, AML, and global regulatory mandates without rebuilding their stack. Authentication becomes not just a safeguard, but a strategic enabler of trust, growth, revenue, and compliance.

Talk to an Identity Expert

See how Entrust unifies authentication across your entire digital ecosystem, delivering seamless, secure experiences for every user, every time. Connect with an Entrust expert today.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

©2026 Entrust Corporation. All rights reserved. Entrust, Datacard, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. PK26Q3-modern-authentication-customer-experiences-sb

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

ENTRUST
SECURING A WORLD IN MOTION