Entrust Identity for Consumers

- Enterprise
- as a Service

ENTRUST

SECURING A WORLD IN MOTION

OVERVIEW

Secure digital identities and communications

Secure consumer communications and transactions rely on identity verification and authentication. In the digital world this has traditionally meant only usernames and passwords. Authenticators like an SMS OTP overcome this limitation, but they are prone to social engineering attacks and SIM cloning/swapping. With each data breach costing an average of $3.9M, and stolen credentials being cited as the root cause 80% of the time, this system is woefully inadequate.

At the same time, consumers are changing the way they conduct transactions. The cashless trend is accelerating with digital wallets, making smartphones the “device of choice” for authenticating user identities and validating transactions. E-commerce transactions are forecast to reach $4.2T by the end of 2020, with 73% of sales taking place on a mobile device. The versatility of mobile is so extensive that it not only enables digital identity issuance, but also changes the way we do identity verification, banking, travel, shopping, and more. We are becoming digital citizens, and smartphones are a cornerstone in this transformation.

Entrust Identity for Consumer IAM

Consumer IAM (CIAM) protects, manages, and maintains the digital identities of your consumer base for the purposes of secure communications and transactions. Entrust Identity provides high assurance consumer IAM with multi-factor authentication (MFA) using one or more of the following:

- A mobile OTP (soft token)
- A push notification
- FIDO2 keys for app/portal sign-in
- PKI capabilities to issue digital credentials on personal devices

Entrust Identity ensures strong security by first establishing trust in the user as well as the device before transacting. One of the core challenges of CIAM is keeping consumers secure without introducing too much friction to avoid abandoned applications and carts. Additionally, there are account takeover (ATO) frauds, which cause significant losses to merchants and consumers. Entrust Identity's adaptive risk-based engine addresses this by introducing additional checks when conditions warrant, like a user logging in for the first time from a new device, at an abnormal time of day, or from a different geolocation. The service offers:

- Proven out-of-the-box integrations
- Rich APIs
- A mobile software development kit (SDK)

Entrust Identity for CIAM is available on-premises (Identity Enterprise) as well as in the cloud (Identity as a Service).

HIGHLIGHTS

Entrust Identity for Consumers

Trusted identity solution providing a seamless digital authentication and access experience. Deploy as needed via cloud or on-premises.

Entrust Identity for Consumer IAM at a glance

	Core Use Cases	Deployment
Identity Enterprise	High assurance MFA, strong customer authentication; secure portals; adaptive risk-based authentication; passwordless login; mobile banking; cardless ATM	On-premises
Identity as a Service	High assurance MFA; strong customer authentication; secure portals; adaptive risk-based authentication; native fraud detection; identity proofing; passwordless login; mobile banking; cardless ATM	Cloud

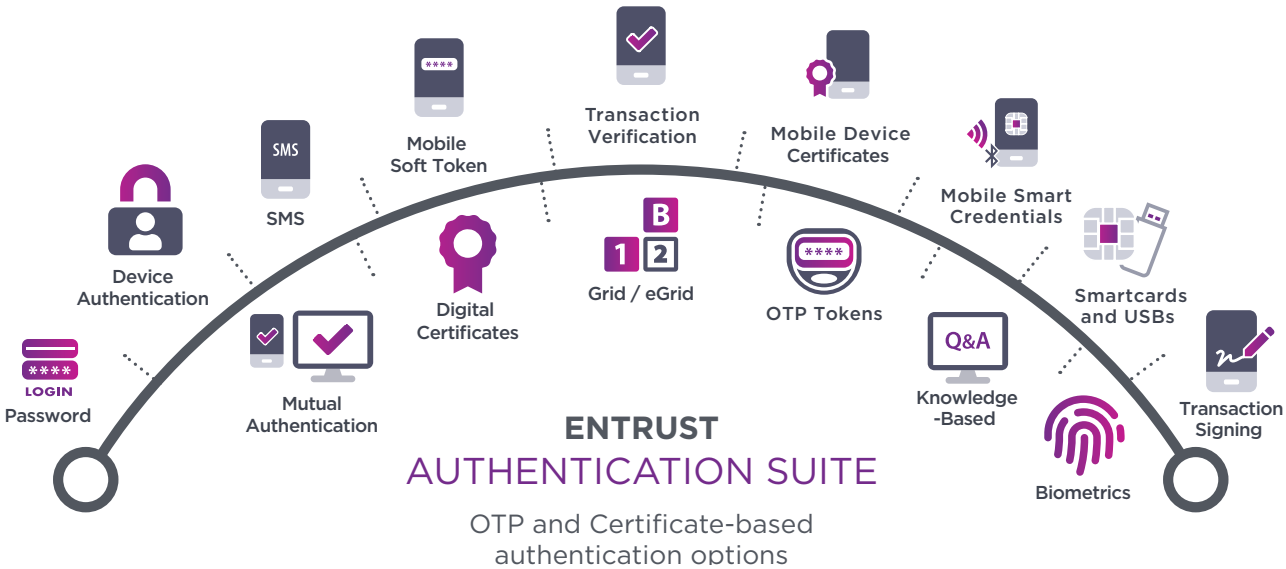
Consumer IAM with Entrust Identity:

- Strong customer authentication for transaction verification
- Secure digital consumer identities
- Minimized user friction for enhanced consumer experience
- Reduced total cost of ownership
- Comprehensive security features, including risk detection
- High scalability and ease of use
- Compliance with industry and geographic regulations

KEY FEATURES

Multi-factor authentication (MFA): Consumers need flexibility for their authentication needs. Usernames and passwords are superseded by 2FA, which has further pivoted us toward multi-factor authentication for stronger security. The consumer wants the ease of using their smartphone, tablet, hardware token, or grid card for accessing different applications and services. Entrust Identity has the widest range of authenticators. These include mobile push, OTP, biometrics (face, fingerprint), deep security features like adaptive (step-up auth and access) techniques based on user risk profiles, trusting the device using a soft token, or native PKI capabilities (issuing digital credentials) that enable high assurance.

Largest number of supported authenticators and use cases



Adaptive risk-based access and authentication: Our solution goes a step further in selecting the right authenticators based on user risk profile and tendencies. Device reputation is an essential element of our adaptive authentication strategy. We apply weightings to the different factors to holistically understand the risk through the policy engine. This is all done pre-authentication to ensure that the transaction request is coming from a legitimate consumer.

Transaction confirmation and non-repudiation: High assurance mobile identity can be used to authenticate across digital and physical channels. User signs into the mobile application using biometrics/PIN, which is verified by soft token/digital certificate/OTP/mobile push. Contextual analysis is maintained throughout the transaction session. Whether a transaction is done using a smartphone or PC, or at an ATM, branch, or call center, we provide non-repudiation protocols (challenge response tokens, verified digital signatures) to prevent fraud.

Self-service password reset: Entrust Identity provides the ability for users to securely reset their own passwords, meaning no downtime.

Email and document signing: Encryption of emails and digital documents is available with Entrust Identity. Adding encryption with authentication strengthens data protection. Document signing also should be secured by using multi-factor authentication to eliminate the risk of impersonation.

Compliance enablement: A comprehensive policy engine controls the compliance aspects of the offering. Region- or industry-specific regulatory compliance (e.g., PSD2, GDPR) policies for strong customer authentication are built in.

Secure portals: Seamless authorization to gain access to customer portals. Extensive integrations with existing CIAM solutions and web apps using rich APIs, SDKs, and developer toolkits. All of this is included out-of-box.

Passwordless access: For a better user experience with security, it is important that authentication solutions move away from passwords. Entrust Identity allows consumers to authenticate their identities by issuing digital certificates (PKI-based smart credential) on their device of choice (smartphone/tablet). This serves the purpose of provisioning a secure identity on a trusted device. User may use biometrics (face, fingerprint, etc.) on mobile to seamlessly log into the apps. Another option is to allow consumers to use FIDO2 keys for passwordless authentication. Passwordless dramatically reduces the complexity for consumers. Instead of remembering multiple passwords, they simply do a few gestures (a swipe, a tap, etc.), which is enough to authenticate themselves.

HOW IT WORKS

Mobile-first approach

The Entrust Identity CIAM solution establishes mobile as a trusted device by bringing together a layered security model. Smartphones are considered a “device of choice” by consumers and offer a lot of functional features:

1. Seamless connectivity to consumer platforms and applications using Bluetooth/biometrics/push notifications

2. Secured transactions for mobile banking, digital wallet, payments (POS/online), and more

3. A way to authorize and sign contracts (digital document signing)

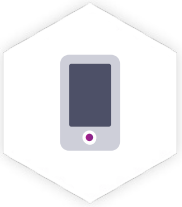
4. A computing platform for threat detection and security improvements

We have extensive experience in this area, with over 100 million mobile credentials issued across industry segments. To secure consumer access, the solution also offers a mobile SDK and APIs, all included out-of-box.

We are well-respected for our authentication offerings by industry experts as well. Entrust Identity is ranked No. 1 in consumer authentication by KuppingerCole in its 2019 Leadership Compass report.

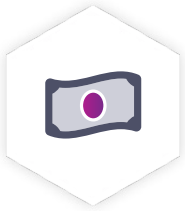
Entrust Identity for Consumers: Use Cases

eGovernment



Virtual Banking and Insurance

Connection to Government Services



Payments

Digital Credentials

Data Protection

Entrust Identity is a comprehensive security solution catering to multiple verticals and user types. Our competency is verifying, provisioning, and authenticating the user identity, along with providing seamless access to applications or portals. Also, Entrust Identity secures the transaction process through advanced features like adaptive risk-based access, digital signing, and encryption. Users can be students enrolling for educational programs, people buying insurance policies, frontline healthcare workers having touchless access, or consumers using their smartphones to make online purchases.

Industry-specific use cases:

Banking: The traditional banking infrastructure is undergoing a complete overhaul. Gone are the days when one needed to be physically present for a credential and identity check. Up to 70% of new account applications are abandoned before completion due to friction in the customer onboarding process (Aite Group, 2019). The industry is being disrupted by the advent of mobile-driven neo-banks and challenger banks. These modernized setups with a technology-first approach not only ensure a good consumer experience, but also implement robust security practices to manage fraud (KYC and AML compliance).

Government: Digital transformation has led governments across the world to ramp up their engagement efforts with their citizens. Approximately 1.1 billion people worldwide have no ownership over their identity. Those who have IDs issued have no control over their identities. Companies holding citizen data are subject to frequent hacks, resulting in extensive data and financial losses. Secure digital credentials for all citizens is an important government initiative, and massive investment and development is being done in this regard. There is extended functional integration with:

- ICAO standards for travel-related documentation like e-Passports
- Mobile driver's licenses and digital national ID issuance platforms
- Citizen portals for permit issuance
- Payment verification systems

Entrust Identity solution matrix for consumer IAM

Feature List	Identity as a Service	Identity Enterprise
MFA	✓	✓
Strong customer authentication	✓	✓
Passwordless access with phone biometrics	✓	✓
Adaptive risk-based access	✓	✓
Identity proofing	✓	✓
Self-service password resets	✓	✓
Device reputation	✓	✓
Email and file encryption	✓	✓
Multi-tier and multi-tenancy	✓	
Document signing	✓	✓
Secure portals	✓	✓
Transaction confirmation & non-repudiation	✓	✓
Mobile SDK	✓	✓
Native fraud detection	✓	
Number of users	0-Unlimited	>5000
Deployment	Cloud	On-Premises

Identity Proofing

> **By 2025, organizations that have undergone a digital transformation initiative putting their customers' identity proofing interests first will reap measurable benefits – 20% more revenue and/or 20% reduced support costs – than competitors mired in a tired and outdated analog identity verification model.**
>
> Jay Bretzmann, Program Director (Security) at IDC

Industry-wide applications and diverse use cases

Banking | Retail | Workplace | Government | Healthcare | Travel

Account opening | Customer onboarding | Age verification | Card transactions | Employee onboarding | Fraudulent ID detection | ePassports | Driver's licenses

Secure Self-Service Identity Verification

Capture and Classify

World-class patented image capture that automatically crops and detects document type, region, and prevents glare.

Facial Recognition

Two classes of facial recognition and liveness tests.

Authentication

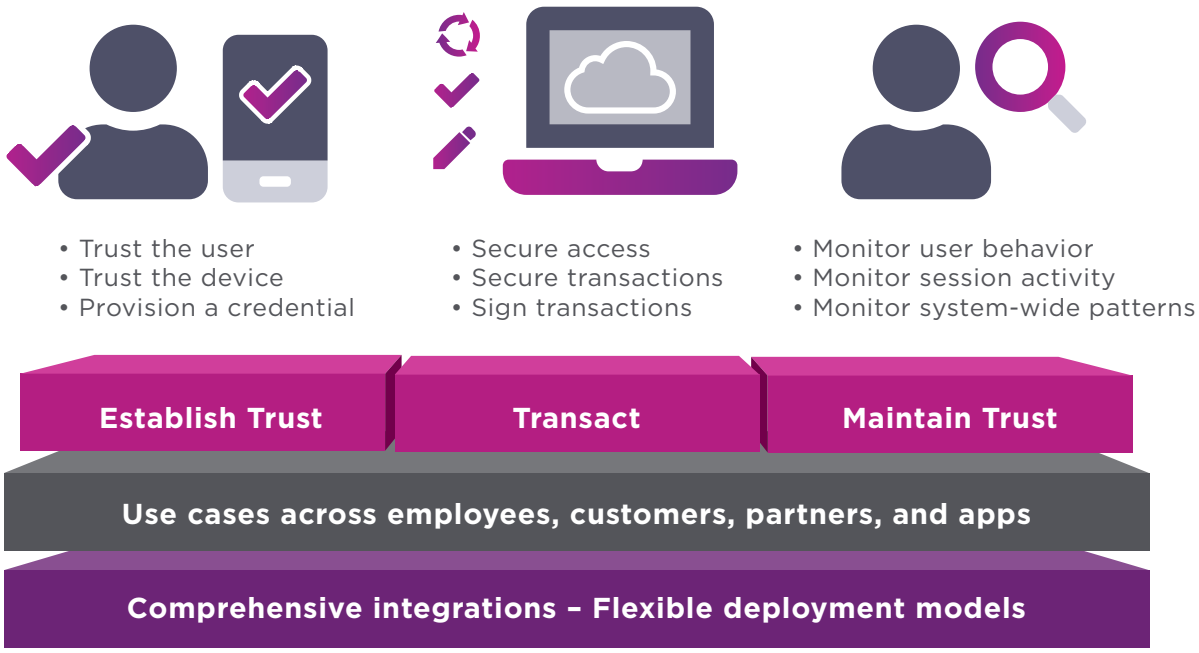
Accurate data population with 50+ forensic tests run in seconds in the same seamless process.

Identity proofing is part of the integrated Identity solution portfolio for consumers that also includes full PKI, smart card, USB, mobile smart credential, digital certificates, document signing, and encryption. Learn more about identity proofing at entrust.com/identity-proofing

OUR OFFERING

Entrust Identity portfolio

Entrust Identity is the IAM portfolio that provides the flexibility and scalability you need to stay ahead of the ever-evolving threat landscape and realize a Zero Trust framework. Beyond consumer and citizen IAM, Entrust Identity also supports workforce use cases. Get started with the use cases and deployment model that makes sense for you today and keep your options open for the future. Entrust Identity is all about ensuring only the right people have access to the right resources.



Flexible deployment, broad capabilities

Entrust Identity can be deployed in the cloud or on-premises. As well, Entrust works with managed service providers to deliver Entrust Identity as a managed service.

Entrust Identity:

- Complements your existing IT infrastructures and workflows vs. seeking to replace
- Delivers the widest support of cloud and on-premises based applications
- Provides the option for digital credential issuance using a soft token or PKI on the mobile device for stronger authentication, which also supports passwordless login with phone biometrics
- Offers a mobile platform with one modern unified app that works across the portfolio
- Provides available out-of-the-box integrations, SAML/OIDC, and APIs
- Includes a mobile development kit so you can embed authentication directly into your own apps and brand as your own
- Offers access to the industry's largest MDM ecosystem, including Microsoft Intune and MobileIron
- Ensures easy IT implementation and efficient operation with point-and-click provisioning, policy management, and self-service password resets

THE ENTRUST DIFFERENCE

A leader in IAM

With 25+ years of digital identity expertise and 50+ years of security innovation, Entrust is an identity and access management leader. Our high assurance solutions are proven with Fortune 500s and governments and are deployed by 10K+ customers around the globe. Entrust Identity secures digital identities and corporate assets, while also improving workforce productivity and removing friction for consumers and citizens.

References

1. IBM Security and Ponemon Institute Cost of a Data Breach Report 2020
2. Verizon 2020 Data Breach Investigations Report
3. Statista March 2018 infographic, Mobile e-Commerce is Up and Poised for Further Growth
4. Dashlane 2015 infographic, Online Overload: It's Worse Than You Thought
5. World Bank Group Identification for Development (ID4D) Global Dataset, June 2018
6. Aite Group June 2019 report, Account Opening: Run It Like You Own It

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com