Entrust Datacard™

+1-888-690-2424

entrust@entrust.com

entrust.com/financial-institutions

@EntrustDatacard

+entrust

/EntrustVideo

/EntrustSecurity

DOWNLOAD THIS DATA SHEET

Layered Security for Financial Institutions

Behavior-Based Security for Customer Identities & Transactions

As global financial institutions seek to grow their customer base and the bottom line, each must increasingly combat sophisticated cybersecurity threats while navigating the growing challenge of compliance risk.

Entrust's identity-based security solutions are specifically tailored to protect financial institutions and the identities of their customers. Strong authentication, real-time fraud detection and comprehensive transaction monitoring are cornerstones to a real solution FIs can deploy — today.

Cross-Channel Security

From wholesale, retail and investment banking to the needs of internal employees, FIs seek to decouple authentication and fraud detection from applications. Implementing cross-channel and cross-application frameworks not only meets varied needs, but provides the agility and flexibility to react to new fraud vectors and compliance regulations.

▶ **entrust.com/financial-institutions**

Mobile Wins Customers, Improves Business

To effectively mitigate risk, enable true efficiency and satisfy customers in the mobile environment, FIs must properly secure mobile devices — but in a way that minimizes user barrier and frustrations. Once secured, leverage mobile devices to improve security, build trust and win customers.

▶ **entrust.com/mobile**

Total Security Framework

Siloed applications and complex IT networks have mushroomed with "islands" of authentication and fraud detection solutions. Entrust's proven authentication and policy framework spans user needs across lines of business, geographies and internal employee controls, helping secure multi-channel transactions, internal systems and applications.

More than 'One-Step' Security

More than one-step security, Entrust's comprehensive framework provides strong protection for customers across varied lines of business and internal employees. Evolve security across multiple access channels (e.g., mobile and online) to provide end-users with a seamless, powerful solution that helps enhance an FI's market position.

Solution Benefits

- Layered security that spans global needs for strong authentication and real-time fraud detection — all in a single security framework
- Unmatched deployment flexibility across user groups, channels, geographies and varied IT network constraints
- Includes comprehensive migration capabilities to co-exist with current systems, streamline transition and reduce overall costs
- Defend against advanced fraud threats and comply with today's global compliance regulations (e.g., Red Flags Rule (FACTA), FFIEC, Faster Payments)
- Provides out-of-band authentication and transaction verification to stop advanced malware, including ZeuS, SpyEye and Ice IX
- Unmatched innovation, breadth of authentication and fraud detection capabilities

Layered Security for Financial Institutions

Behavior-Based Security for Customer Identities & Transactions

Entrust Multilayered Security Approach

Entrust's multilayered approach leverages advanced security technology that are already successful for today's top financial institutions.

Strong Authentication

One of the pillars of the Entrust solution, risk-based authentication identifies situational risks and adapts in real-time. And Entrust's comprehensive line of authenticators may be managed on a single platform, providing the versatility to adapt as threat vectors evolve.

Fraud Detection

Real-time fraud detection monitors both user and Web-access behavior for 360-degree insight to advanced fraud attack vectors. This visibility also provides the data necessary for step-up authentication to increase security during risky or suspicious transactions.

Transaction Verification

Leverage out-of-band channels, including mobile devices, to increase security during online transactions. Asking customers to verify transactions — either all or those that meet a certain risk threshold — greatly reduces the success of fraud attacks. This technique is particularly adept at stopping man-in-the-browser malware attacks.

Simplifying Architecture

Based on geographic location, customer type, transaction amounts, or even nation and global regulatory mandates, financial institutions have unique requirements for authentication frameworks.

Unfortunately, in many cases, these frameworks are tied to a specific application, location or even user-group. Entrust helps financial institutions consolidate authentication technology across an entire enterprise. This smart approach helps solve the biggest challenges of today's security-conscious FIs.

Empowerment Through Security

Ensure Compliance — Adapt to various domestic and international regulatory requirements like FFIEC, Red Flags Rule, etc.

Satisfy End-User Needs — Meet authentication needs of diverse end-user groups (e.g., retail, wholesale, high-net worth).

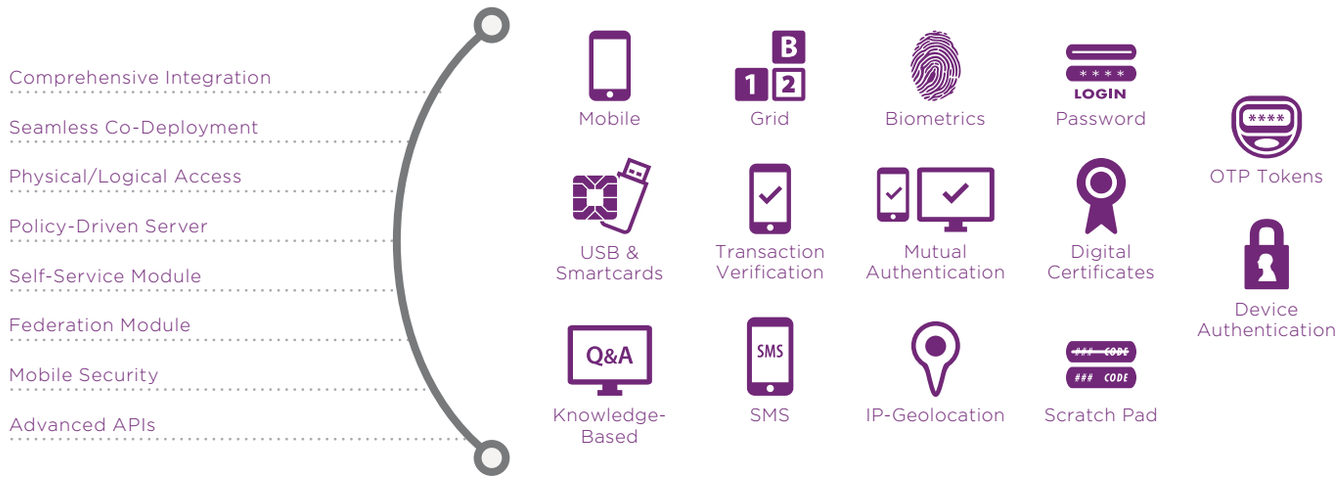
Meet Multichannel Requirements — Meet authentication needs of various channels, particularly emerging platforms like mobile and cloud.

Empower Global Workforce — Integrate a single authentication management platform to provide physical and logical access for global enterprise security.

Simplify Risk Management — Platform versatility enables quick migration to different authenticators.

Reduce Costs — Consolidating platforms and working from a common security policy framework streamlines security management and reduces the total cost of ownership.

Entrust IdentityGuard Transaction Verification - How it Works



Entrust IdentityGuard: Enterprise-Wide Authentication Framework

The Entrust IdentityGuard software authentication platform is a comprehensive security framework that serves as the foundation of a complete, layered security environment.

Entrust's management framework is unique in the market and drives significant value for financial institutions. The solution enables organizations to deploy strong, risk-based authentication to properly secure banking customers.

- Deploys to a single server
- Co-deployment with existing authentication measures
- Simple integration and easy-to-use APIs
- Mobile, physical and logical authentication
- Federate internal and cloud-based applications (e.g., Salesforce.com, Microsoft 365)
- Reduce cost and maximize staff efficiency with an intuitive self-service module

Emerging Paradigms: Mobile Devices, Tablets & Cloud

With financial institutions placing great emphasis on the security of customer identities and transactions, they've also been purposely cautious when leveraging new platforms or technology like mobile devices, tablets and cloud services.

Entrust helps eliminates security risks on emerging platforms by delivering proven capabilities that embrace innovative technology and provide enhanced convenience to end-users — all without sacrificing security.

Embrace New Technology

Federation Capabilities — Provide secure single sign-on (SSO) to cloud services and applications.

Real-Time Transaction Safeguards — Approve large-value payments or set up sweeps for a superior client experience.

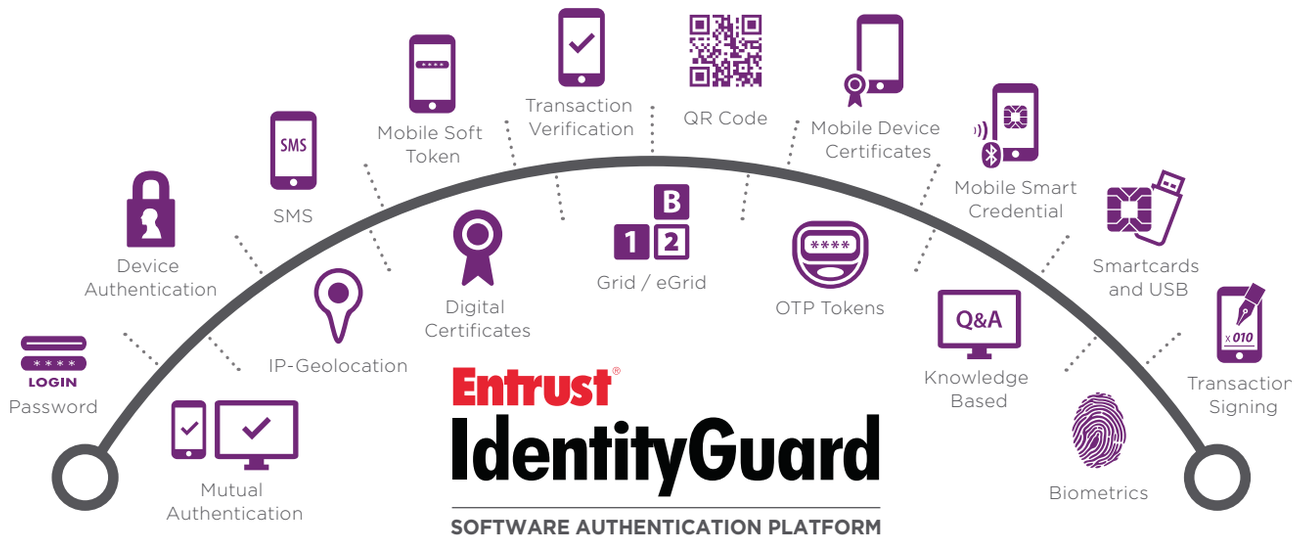
Mobile Technology — Leverage mobile devices and tablets as a strong authenticator to secure transactions and defeat advanced malware.

Application Security — Provide strong authentication for both internal and cloud-based applications.

Layered Security for Financial Institutions

Behavior-Based Security for Customer Identities & Transactions

Software Authentication Platform



Powered by Entrust IdentityGuard. The widest range of authenticators on the market today — all from a single platform.

True Risk-Based Authentication

As online fraud increases in sophistication, organizations need to deploy proven solutions that help manage identity credentials — at both the initial login and throughout the session. As the risk of a transaction elevates, so should the strength of authentication. It's important to remember, however, that a one-size-fits-all approach to authentication is not appropriate for most customer or business-banking environments.

The Layered Approach

Entrust enables organizations to layer security — according to access requirements or the risk in a given transaction — across diverse users and applications.

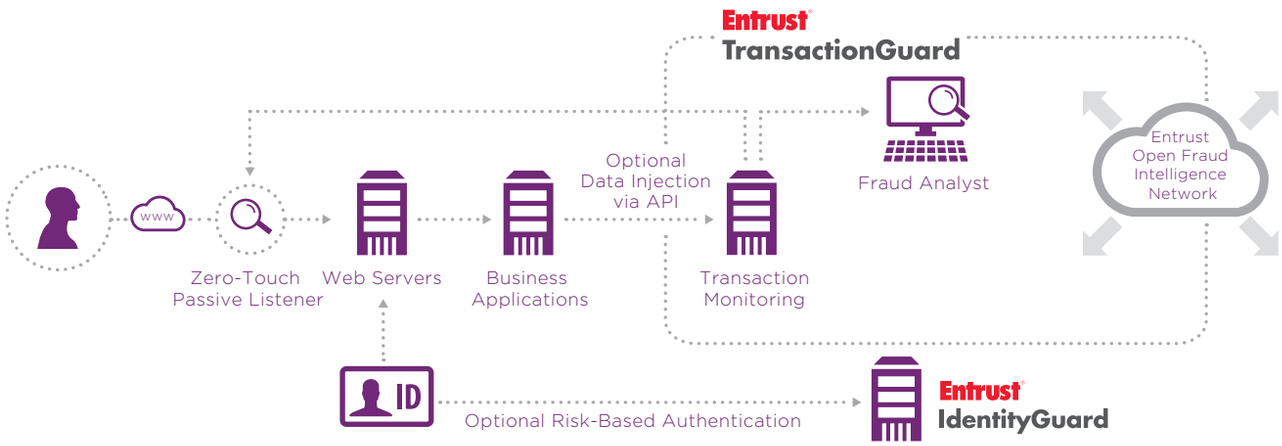
Entrust's software authentication platform does not impact normal user behavior or back-end applications, speeding deployment and helping to save money.

Custom Authentication

The use of specific authenticators may be defined via back-end policies that can be tailored per applications and/or groups.

A simple policy change may seamlessly adjust the authentication behavior of all applications — instantly with no front-end changes. Financial institutions may even mix and match authenticators depending on specific customer needs.

Real-Time Fraud Detection Architecture



Comprehensive security for FIs. Entrust provides a proven architecture that delivers real-time fraud detection, risk-based authentication and critical information-sharing capabilities.

Entrust TransactionGuard Integrating Real-Time Fraud Detection

Entrust TransactionGuard has evolved from a real-time, transaction-monitoring system to a state-of-the-art platform that blends a number of approaches to form a true fraud model. This helps financial institutions detect fraud without invasive integration with existing online applications, empowering organizations to quickly bring new applications to market without concern over the impact of fraud monitoring.

Unlike competitive offerings limited to transaction-based fraud detection, Entrust TransactionGuard analyzes all points of interaction across multiple channels, allowing organizations to gain a complete picture of potentially fraudulent behavior.

Alerts & Reporting

High-risk transactions are managed according to business procedure and the level of risk in real time. Alert generation, case reporting and workflow tools enable an organization to investigate and stop fraudulent transactions before they clear or approve legitimate business, without impacting the user — all necessary tools to help stop man-in-the-browser attacks.

Comprehensive Fraud Monitoring

This proven solution provides detailed “front-door” monitoring from the moment a user interacts with a specific channel to full “in-session” analysis with the ability to monitor both transactional data and underlying HTTP(S) access data.

This information includes navigation speeds and patterns, IP address anomalies, and even detection of user-agent strings and HTML-injection attacks.

Rich API Abilities

For organizations with challenging data center requirements, application nuances or a need to integrate external system data, Entrust TransactionGuard supports rich fraud APIs that enable transactional data, external feeds or third-party fraud alerts to be injected into the fraud model.

Step-Up Security

Entrust provides real-time protection by transparently monitoring user behavior to identify anomalies, then calculating the risk associated with a particular transaction. If a risk is identified, step-up authentication can be required — leveraging Entrust IdentityGuard — to complete the transaction.

Flexible Deployment & Migration

One of the most critical challenges of bank security is upgrading or migrating to new solutions to help address evolving attack vectors and defending against sophisticated malware trends. It's important that a new authentication framework easily integrates into existing application infrastructure.

On-Premise Model

Deploy mobile-based, one-time passcodes (OTP), grid cards or SMS OTPs to strongly authenticate identities that require two-factor access controls to either customer-facing or enterprise-based Web applications.

Seamless Co-Deployment

Understanding that FIs can't realistically remove an existing security solution, Entrust streamlines migration with a proven, co-deployment model that helps reduce challenges during transition.

This rich deployment flexibility is built into a solution platform over time. Entrust's integration expertise is born from collaborating with the world's most trusted FIs for years, then defining the capabilities that enable proper deployment.

Mobile Security

Entrust IdentityGuard enables financial institutions to leverage mobile devices to achieve greater efficiency in all environments. Entrust provides mobile security capabilities via distinct solution areas — mobile device authentication, transaction verification, mobile smart credentials, and transparent authentication technology with an advanced software development kit.

These Entrust IdentityGuard capabilities help organizations and financial institutions strongly authenticate consumer and business customers without requiring specialized security hardware such as one-time-passcode (OTP) hardware tokens.

Broad Platform & Integration Support

Entrust IdentityGuard features software-based, one-time-passcode authentication on today's leading smartphone platforms, including Apple iOS, Google Android, Windows Phone and BlackBerry. Select platforms also gain out-of-band transaction verification to help combat online fraud — a seamless, back-end experience that doesn't require the user to enter a confirmation code to complete a transaction.

Easy-To-Use SDK

Entrust's easy-to-use software development kit (SDK) helps you create customized mobile authentication applications tailored to the requirements of your specific environment.

Soft Tokens

Reduce strong authentication costs by leveraging existing devices. Entrust places soft tokens on smartphone platforms to improve end-user adoption and simplify the authentication of identities. Further simplify deployment with easy over-the-air activation (OTA) via the Entrust IdentityGuard Self-Service Module or a Web link distributed via email.

Alert Notifications

Entrust IdentityGuard supports push notifications to mobile devices alert users of a pending transaction. This helps quickly notify users of potential fraud.

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Entrust Datacard™
Trusted Identities | Secure Transactions

22605/4-15