Entrust® Securing Digital Identities & Information

SECURITY ON

Layered Security for Financial Institutions

Enterprise-Wide Authentication & Fraud Detection Framework

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 related to adhering with in-country laws.

Compounding the problem, siloed line-of-business applications and complex IT networks have mushroomed with "islands" of authentication and fraud detection solutions throughout the enterprise.

To effectively improve security and compliance controls, total cost of ownership and the end-customer experience, the world's top financial institutions are adopting identity-based security and fraud detection platforms that span enterprise-wide needs.

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.

Enterprise-Wide Security Framework

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

This is achieved on a proven authentication and policy framework that spans user needs across lines of business, geographies and internal employee controls, helping secure multi-channel transactions, internal systems and applications.

Multilayer Security Approach

Entrust provides more than a simple one-step means of protecting the world's largest and most respected financial institutions.

This unique layered strategy enables financial institutions to quickly deploy and build a security framework that not only provides strong protection for customers across varied lines of business but also evolves 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.

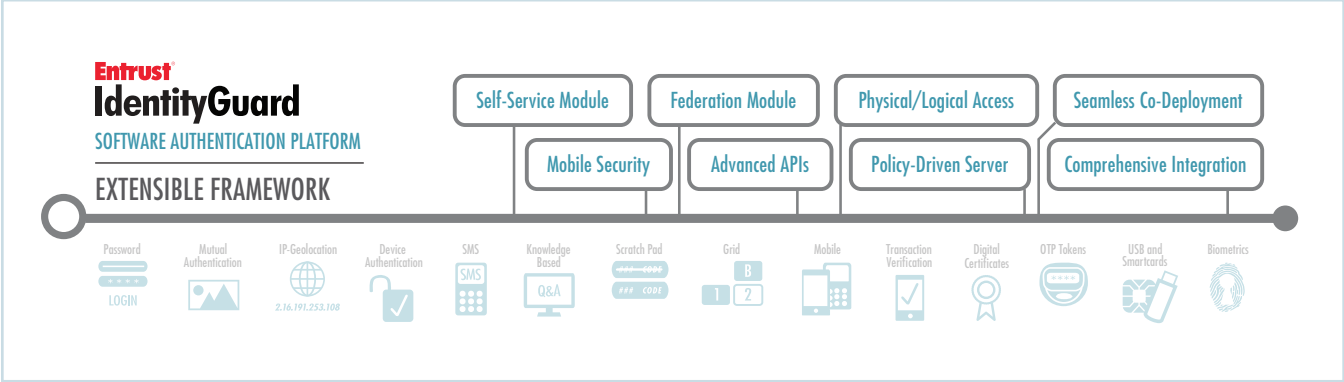
Solution Benefits

- 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
- Empowers FIs to defend against advanced fraud threats and comply with today's global compliance regulations (e.g., Red Flag (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

Entrust Multilayered Security Approach *Entrust's multilayered approach leverages advanced security technology that are already successful for today's top financial institutions.*		
Strong Authentication	**Fraud Detection**	**Transaction Verification**
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.	Real-time fraud detection monitors both user behavior 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.	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.

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. The solution enables organizations to deploy strong, risk-based authentication to properly secure banking customers.



Entrust's management framework is unique in the market and drives significant value for financial institutions. This approach not only helps manage all authentication needs, but also provides capabilities unique to the market.

- 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

SIMPLIFYING ARCHITECTURE

Based on geographic location, customer type, transaction amounts, or even national 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.

Compliance — Adapt to various international regulatory requirements like FFIEC, Red Flags, etc.

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

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

Empowering 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.

EMERGING PARADIGMS: MOBILE DEVICES, TABLETS & CLOUD

With financial institutions placing great emphasis on the security of customer identities and transactions, they're also 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.

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 advance malware.

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

FLEXIBLE DEPLOYMENT & MIGRATION

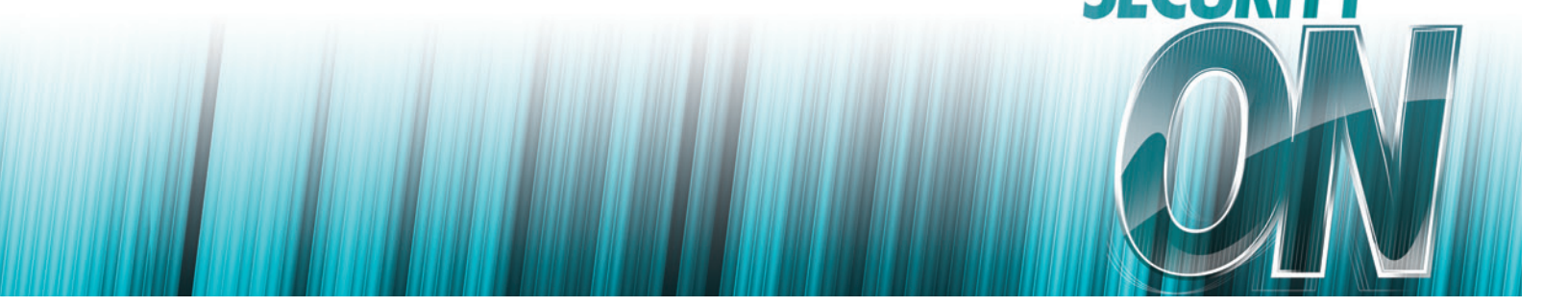
One of the most critical challenges of bank security is upgrading or migrating to new solutions to help address evolving attack vectors and defending against sophisticated malware trends. It's important that a new authentication framework easily integrates into existing application infrastructure.

Entrust's complete solution is offered in an on-premise model and provides customers with a range of deployment options to meet the needs of the most complex IT architecture.

In fact, both Entrust TransactionGuard and Entrust IdentityGuard incorporate native server-redundancy and disaster-recovery capabilities, and meet the most demanding scalability requirements across a range of disparate user groups, business applications and geographic locations.

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.



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.

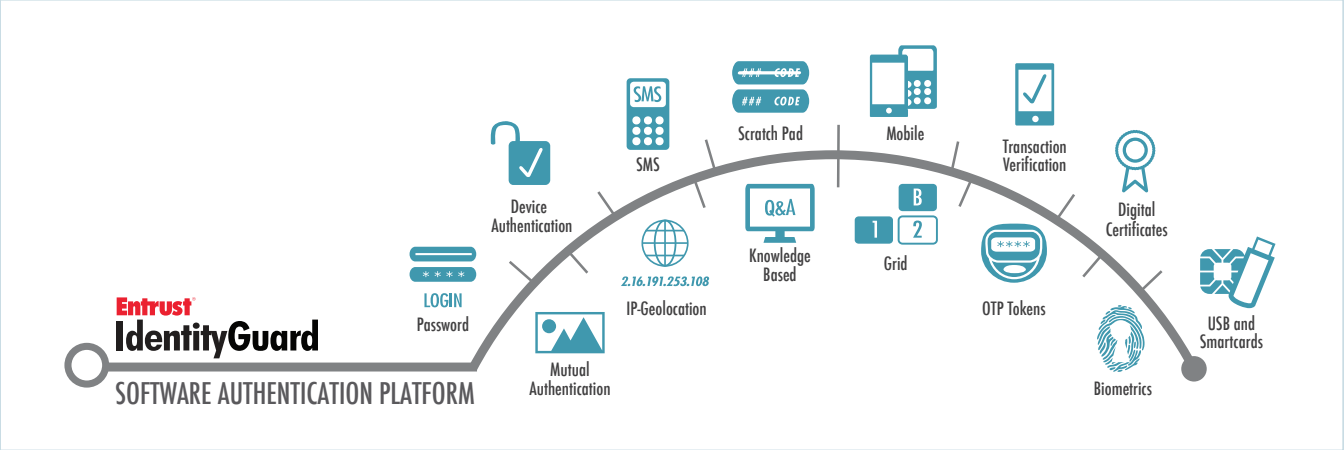


Figure 1: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today.

DEFENDING AGAINST MAN-IN-THE-BROWSER MALWARE

Entrust's comprehensive identity-based approach leverages the Entrust IdentityGuard software authentication platform and the Entrust TransactionGuard fraud detection solution to deliver multiple proven methods for defending against man-in-the-browser attacks, including such variants as ZeuS, SpyEye and Ice IX.

Leveraging Secure Channels

Entrust helps defeat man-in-the-browser attacks by leveraging a different channel than the one being compromised. Online- or mobile-banking applications integrated with Entrust IdentityGuard can notify a user's smartphone to retrieve transaction details from their bank. The user may then verify the actual transaction details and decide whether or not to acknowledge.

If the transaction is being tampered because of a compromised desktop, the user may see it and immediately stop the transaction, defeating the man-in-the-browser attack.

In cases where the transaction is legitimate, a transaction signature is generated by Entrust's mobile application. This ties the transaction to the user's identity, ensuring the bank the processing transaction is acknowledged by the user.

Real-Time Fraud Detection

An integrated zero-touch, risk-based approach, Entrust's fraud detection platform helps defeat man-in-the-browser by analyzing transaction behavior and blocking transactions or stepping-up authentication if such behavior is considered slightly abnormal — all in real time.

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.

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.

Zero-Touch Integration
Quickly introduce new applications and start monitoring fraud rapidly. With a proven zero-touch approach, there's no software to deploy and direct integration to banking applications is unnecessary.

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.

Proactive Safeguards
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.

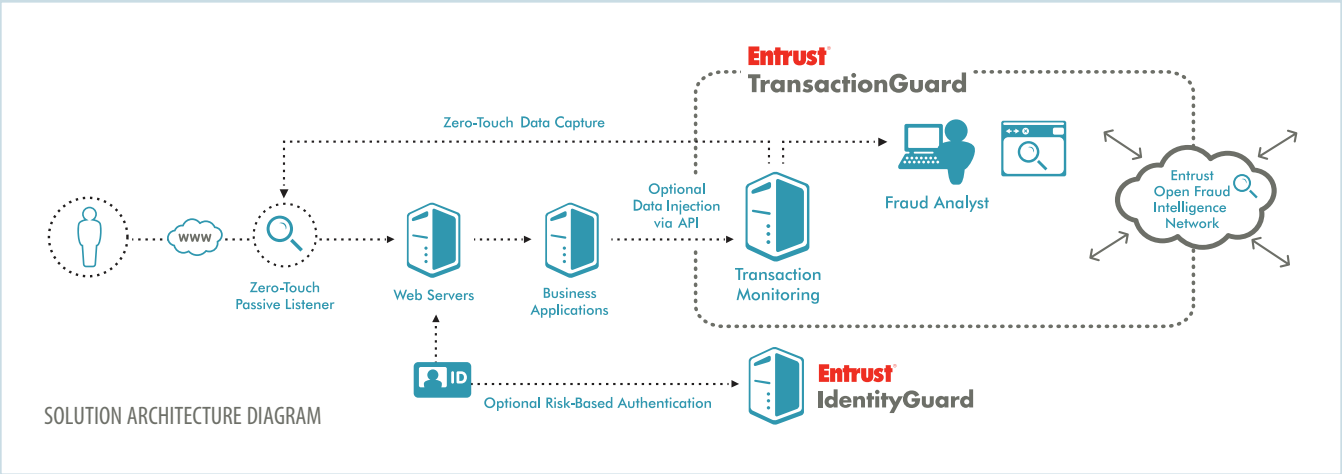


Figure 2: Entrust provides a proven architecture that delivers real-time fraud detection, risk-based authentication and critical information-sharing capabilities.

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, as well as out-of-band transaction verification, on today's leading mobile platforms, including Apple iOS, RIM BlackBerry, Google Android and Microsoft Windows Mobile (6.0-6.5).

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.

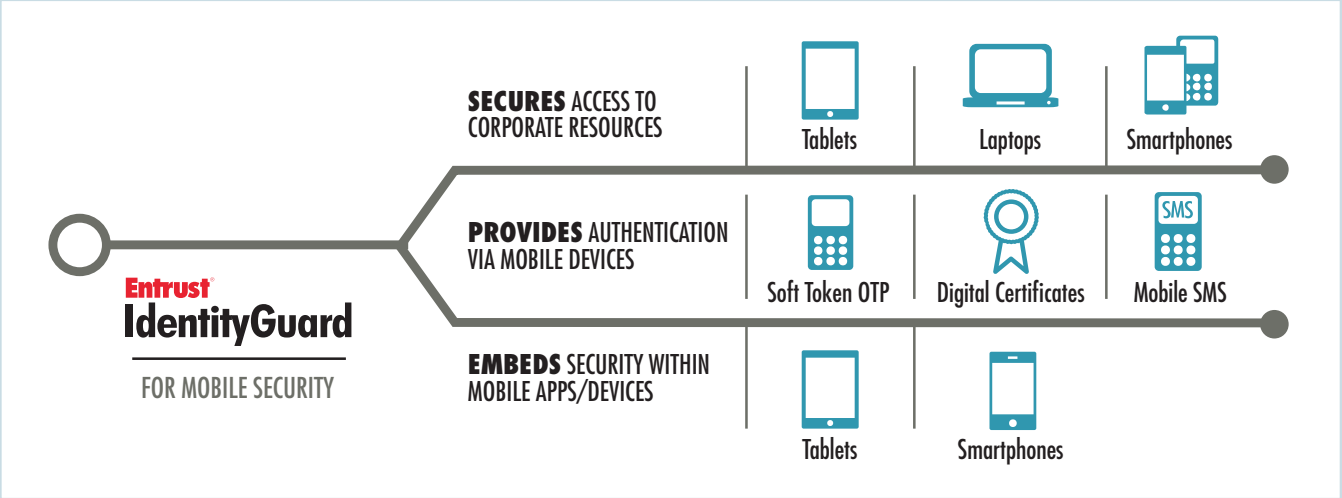


Figure 3: Entrust IdentityGuard helps financial institutions leverage the convenience of mobile devices in a manner that is safe, secure and reduces opportunity for attack.

More Information

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service. Discover how this will benefit you by contacting us at **888.690.2424** or via email at **entrust@entrust.com**.

About Entrust
A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Entrust® Securing Digital Identities & Information

22605/5-12