



< Let's Talk

Strong Authentication & Fraud Detection

Security Solutions for Customers & Corporate Banking

Identity theft and online fraud, specifically targeting customers and business-banking accounts, continue to accelerate at an alarming rate. By leveraging social engineering and the latest in malware technology, including man-in-the-browser attacks, today's online threats are increasingly sophisticated and effective.

Organizations conducting online business — particularly financial institutions serving customers and business-banking customers — have come under an increasing number of attacks because of the potentially lucrative rewards for online criminals.

Entrust — Identity-Based Security

Entrust solutions empower individuals, enterprises and governments by securing identities based on a defined role and the security level appropriate for a given transaction of funds or information.

Whether defending against social engineering techniques or advanced malware attacks, Entrust's identity-based approach ensures a comprehensive solution for securing sensitive customer and business financial environments.

More Authenticators, One Platform

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.

Multilayered Security

Entrust enables organizations to layer security — according to access requirements or the risk in a given transaction — across diverse users and applications. Entrust's versatile authentication platform does not impact normal user behavior or back-end applications, speeding deployment and helping to save money.

Versatile Authentication

The solution's authentication capabilities include username and password, IP-geolocation, device, questions and answers, out-of-band one-time passcode with transaction details for verification (delivered via voice, SMS, e-mail or Entrust IdentityGuard Mobile), grid and eGrid cards, digital certificates (in software or on smart cards/USB Tokens) and a range of one-time-passcode tokens.

Solution Benefits

- Combines award-winning versatile authentication platform with market-leading real-time fraud detection — all in a single solution
- Widest range of authenticators available on a single platform
- Provides three proven methods for helping defeat man-in-the-browser (MITB) attacks
- Behavioral and transactional fraud detection, implemented in real-time, with no impact on applications or the user experience
- Cost-effective, proven solution that can be deployed to large customer and business environments
- Helps comply with today's consumer-based compliance regulations (e.g. Red Flag (FACTA), FFIEC, Faster Payments)
- Trusted by leading organizations like Schufa, CommerceBank, Bank of New Zealand, the Government of Sweden and more

Entrust also provides multiple methods of supporting mutual authentication, including picture and caption replay as well as multi-domain Extended Validation (EV) SSL certificates.

Defeating Man-in-the-Browser

One of the most complex forms of malware used by criminals today, a man-in-the-browser (MITB) attack typically takes the form of an invisible browser extension, installed unknowingly by the user as a result of social engineering (e.g., phishing). From the user's point of view the Web transaction takes place normally, complete with expected interactions with the organization's Web site.

The malware modifies Web sessions at will and initiates fraudulent transactions — all while showing the session as normal to the user, making it next to impossible for an end-user to detect. Whether a consumer or a business-banking customer, the impacts can be devastating.

Unfortunately, today's antivirus applications — and even some authentication methods — can't stop the onslaught of man-in-the-browser attacks. By offering the proper combination of strong authentication and real-time behavioral fraud detection, Entrust offers three proven techniques to help identify and defend against man-in-the-browser malware.

Mobile Security

Entrust IdentityGuard Mobile is a family of identity applications that leverage mobile devices for greater authentication security. Proven transaction verification, one-time-passcode (OTP) authentication and Entrust's advanced software development kits (SDK) are powerful tools in the fight against online and mobile fraud.

Convenient, Effective

This innovative mobile identity application helps organizations and financial institutions strongly authenticate consumer and business customers by leveraging their existing mobile device, maximizing user convenience.

Popular Platforms

Entrust IdentityGuard Mobile features software-based, one-time-passcode authentication, as well as out-of-band transaction verification, on today's leading smartphone platforms, including the Apple iPhone, RIM BlackBerry, Android, Microsoft Windows Mobile and Symbian (Java).

For Developers

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



< Let's Talk

Integrating Real-time Fraud Detection

Core to an integrated approach for protecting online customer and business users, Entrust TransactionGuard can 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 can analyze all points of interaction with the user on a Web site, allowing organizations to gain a complete picture of potentially fraudulent behavior.

Good Behavior

The solution 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.

You Against MITB

Entrust's comprehensive identity-based approach leverages the Entrust IdentityGuard versatile authentication platform and the Entrust TransactionGuard fraud detection solution to deliver multiple proven methods for defending against man-in-the-browser attacks.

Outside the Channel

Entrust helps defeat man-in-the-browser attacks with out-of-band, one-time-passcode (OTP) authentication with transaction details, which can be delivered through SMS, voice or Entrust IdentityGuard Mobile.

Mobile Convenience

Entrust IdentityGuard Mobile is the most convenient, easy-to-use method to enable strong authentication and helps defeat man-in-the-browser and other malware attacks.

Real-Time Fraud Detection

A zero-touch, risk-based approach, Entrust's fraud detection platform can help defeat man-in-the-browser by analyzing transaction behavior and stepping up authentication when appropriate — all in real-time.

Logical, Versatile

Offering the widest range of authenticators from a single platform, Entrust's proven strong authentication solution can properly match an authenticator with an associated risk or user role — the most secure, cost-effective approach for large customer and business deployments.



< Let's Talk

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

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 e-mail at **entrust@entrust.com**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 4,000
Offices: 10 globally

Headquarters

One Lincoln Centre
5400 LBJ Freeway, Suite 1340
Dallas, Texas 75240 USA

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
E-mail: entrust@entrust.com



About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust® Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2011 Entrust. All rights reserved.