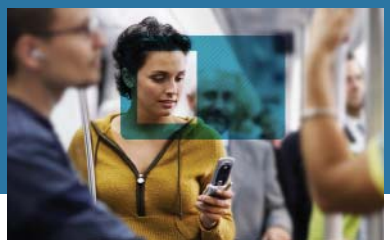
Entrust® Securing Digital Identities & Information



Entrust IdentityGuard Mobile

Mobile Authentication for Stopping Man-in-the-Browser

Identity theft and online fraud, specifically targeting consumers and business 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 criminals are increasingly sophisticated and effective.

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

Defeating Man-in-the-Browser

While there are many safeguards deployed inside financial institutions today, criminals are increasingly turning to highly effective social engineering tactics, combined with stealthy malware, to illegally obtain consumer identities.

Advanced Malware. One of the most advanced 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.

A Proven Approach. Unfortunately, many security methods — antivirus protection, OS-level patching, traditional strong authentication and legacy fraud detection — are simply not effective against man-in-the-browser attacks. And most current solutions that can address the problem tend to be expensive, hard to use and difficult to deploy.

To properly address man-in-the-browser attacks, organizations need to deploy authentication methods that are "out-of-band" from the originating transaction — not on the local computer — as well as including the transaction details for the user to verify before proceeding.

Product Benefits

- Strong mobile authentication with out-of-band transaction confirmation defeats man-in-the-browser
- Leverages existing smartphones to boost authentication strength without inconvenience
- Standards-based (OATH) authentication and signature
- Support for leading smartphone platforms including Apple iPhone, RIM BlackBerry, Symbian (Java) and Windows Mobile
- Customizable to include organization-specific branding for increased user acceptance

Entrust IdentityGuard Mobile

Behavioral and transactional fraud detection can also play a critical role in detecting and defending against man-in-the-browser attacks.

Proven Strong Authentication

Entrust IdentityGuard Mobile, an innovative mobile identity application, helps organizations strongly authenticate customers and employees, without requiring specialized security hardware. The solution delivers unique capabilities that defeat the latest malware threats impacting online-banking users today, including man-in-the-browser attacks that are causing significant losses — and even bankruptcies — for business-banking customers.

Entrust IdentityGuard Mobile enables strong authentication and detailed secure transaction review and confirmation on the handheld device, using a standard software-based, one-time passcode (OTP) on leading mobile devices.

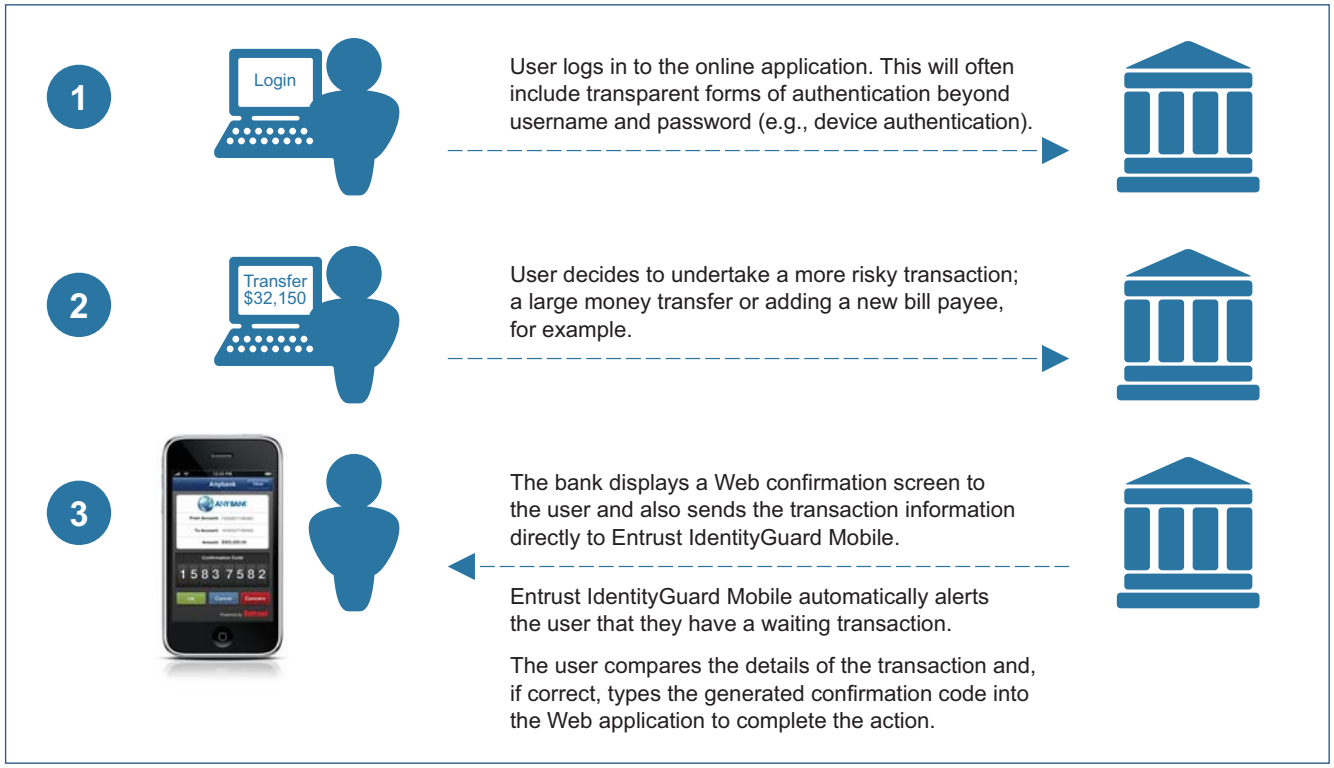
In addition to enabling strong authentication with a software-based OTP token, Entrust IdentityGuard Mobile also provides the ability to strongly authenticate an online transaction, taking into consideration the details of that specific transaction.

Advantages

Secure. The only mobile authentication solution on the market today that addresses the man-in-the-browser malware threat. Key to interoperability, it leverages proven time-based, OATH-compliant OTP authentication and out-of-band transaction verification on leading mobile devices.

Easy to Use. The most convenient, easy-to-use strong mobile authentication method available today, Entrust IdentityGuard Mobile enables out-of-band transaction verification, OATH-compliant signatures and even a method to immediately report suspicious account behavior.

Entrust IdentityGuard Mobile — How it Works



The end-user isn't forced to enter any data within the smartphone application, only a straightforward Web confirmation code to complete the transaction online.

Portable. Enables use of leading smartphones to boost authentication strength by not requiring the user to carry an extra hardware device or have access to a specific computer.

Cost-Effective. Unlike physical options, Entrust IdentityGuard Mobile leverages the user's existing phone; there's no extra physical hardware to buy and deploy.

In addition, Entrust IdentityGuard Mobile delivers transaction notifications directly to the phone without the use of SMS.

Flexible. Supports the use of both simple time-based OTP as well as out-of-band transaction signatures. Also supports multiple identities within the same application, enabling organizations to fully leverage the deployed application (e.g., a banking ID as well as a corporate remote access ID).

Broad Platform Support. Supports the leading mobile smartphone platforms on the market today, including Apple iPhone, RIM BlackBerry, Symbian (Java) and Windows Mobile.

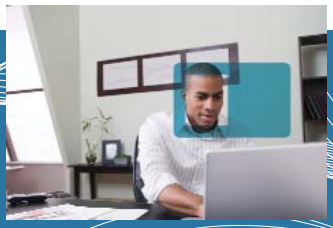
Standards-Compliant. Uses the OATH standard for time-based, one-time passcode and transaction signature generation.

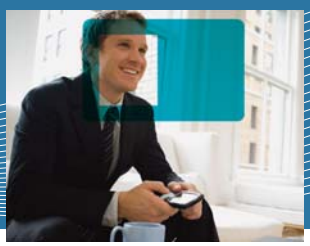
Customizable. Includes the ability to add organization-specific branding to each identity, improving usability and reinforcing brand image.

Entrust Stops MITB Malware

Entrust IdentityGuard Mobile works in conjunction with Entrust's proven authentication and fraud detection solution, which is recognized by leading analyst firms for its ability to stop man-in-the-browser malware.

Entrust is the only vendor that offers three distinct and highly effective ways of addressing man-in-the-browser attacks — behavioral and transactional fraud detection; SMS authentication with transaction details; and mobile out-of-band transaction verification and signature.





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.

More Information

For more information on Entrust IdentityGuard Mobile, contact the Entrust representative in your area at **888-690-2424** or visit **www.entrust.com/mobile**.

Company Facts
Web Site: 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

24003/4-10