Entrust® Securing Digital Identities & Information

SECURITY ON

Mobile Security Solutions

Securing & Leveraging Mobile Devices

The proliferation of mobile devices presents tremendous opportunities for financial institutions and enterprises to provide traditional online activities and services in ways that are more convenient. But as the use of mobile devices and applications grows, so does the rate and sophistication of identity attacks on popular mobile platforms.

Whether it's for banking, online services or Web-based transactions, this shift has forced FIs and global banks to re-think how they service customers.

In contrast, enterprises face a different set of challenges with personal and corporate-issued mobile devices co-existing within secure corporate infrastructures. Today's enterprise is falling victim to unrelenting attacks that specifically target mobile platforms — all in hopes of stealing sensitive data and damaging valuable brand image.

Financial Services & Mobile Security

While many safeguards are deployed within financial institutions, criminals are evolving their techniques rapidly. Phishing, smishing and spear-phishing attacks deploy malware, which take over users' browsers to execute malicious transactions.

The mobile experience is key to financial institutions for augmenting security across channels. Regardless of the type of application — internal, wholesale or retail — leveraging the Entrust IdentityGuard software authentication platform for mobile security ensures a unique, common and secure experience.

Mobile Application Development

With Entrust's easy-to-use software toolkit, it's simple to integrate Entrust IdentityGuard into mobile-banking or transaction-based applications — bringing advanced identity-based security to mobile and online channels.

The SDK enables organizations to seamlessly embed strong authentication into an application's mobile session without requiring the user to input a one-time passcode (OTP). Entrust employs a highly secure, encrypted proprietary protocol between the server and the mobile device, to provide the most secure protection against malicious online threats.

With straightforward APIs, the Entrust IdentityGuard Mobile SDK allows developers to easily design and implement uniquely branded mobile applications without sacrificing usability or transparency for end-user adoption. And with support for Apple iOS, Google Android, RIM BlackBerry and Java platforms, the toolkit delivers a common API framework that allows developers to leverage integration efforts across multiple development environments.

Solution Benefits

- Uses software authentication platform that's core to framework security strategies for financial institutions and enterprises
- Strengthens identity security while offering seamless integration and improved end-user experience
- Leverages core mobile technology including NFC and Bluetooth standards for more convenient physical and logical access via mobile devices in the enterprise
- Secures mobile devices communicating with customer or enterprise environments
- Provides strong, transparent authentication for mobile devices
- Enables use of mobile soft tokens as an easy-to-use authenticator
- Uses transaction verification for additional security and confidence
- Issues and manages digital certificates on mobile devices
- Enables multiple identities to be used on a single mobile device
- Helps FIs defend against phishing and malware, including ZeuS, SpyEye and Ice IX

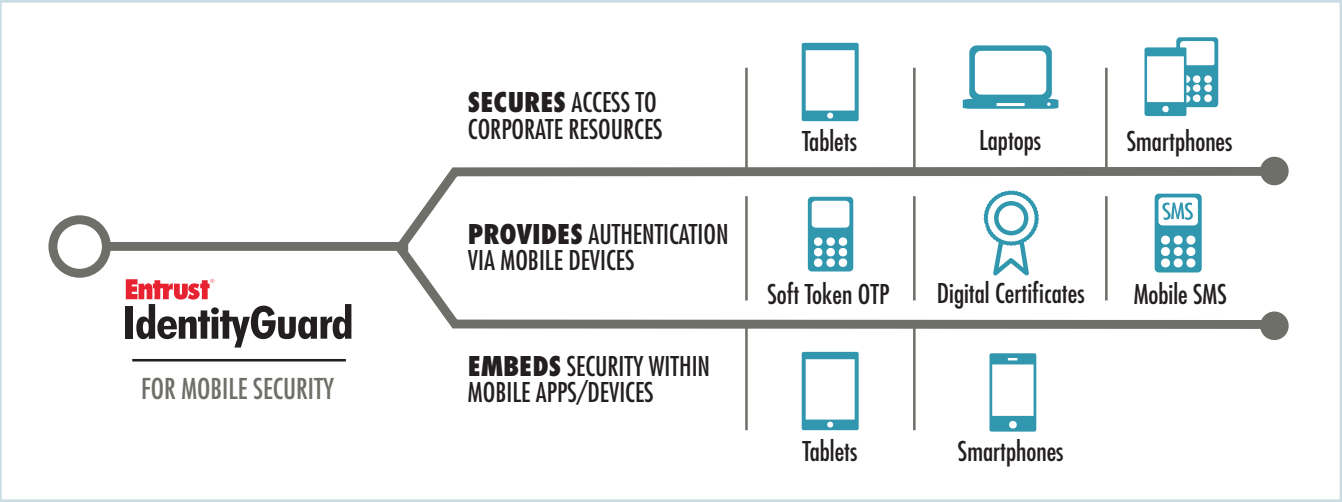

Figure 1: Entrust IdentityGuard helps organizations leverage the convenience of mobile devices in a manner that is safe, secure and reduces opportunity for attack.

Securing Mobile FI Customers

Financial institutions are encouraged to deploy specific security techniques to help protect customers using mobile devices, but extending mobile technology to secure sensitive transactions in traditional online channels is just as critical in the fight against fraud.

- **Mobile Soft Tokens.** A soft token on a user's mobile device is an effective, easy-to-use form of stronger authentication that allows banks to leverage physical devices that are widely deployed.

  This out-of-band OTP is generated on the device and is used in conjunction with an individual's username and password to strongly authenticate an online-banking session. And unlike hard tokens, which have their static unique seeds stored at the backend, a soft token seed is derived and can be modified at any given time.

- **Out-of-Band Transaction Verification.** Banks should also use the mobile channel to notify a user's smartphone of a given transaction. Upon reception of such a notification, the transaction details are securely retrieved out-of-band and displayed to the user who, in turn, may accept or reject the transaction.

  Upon acceptance of the transaction, a unique OTP signature or confirmation code is generated, binding the transaction details to a user's identity. This confirmation code may then be used within a banking application to ensure that the transaction hasn't be tampered with by a compromised desktop.

- **Mobile Smart Credentials.** Banks that require non-repudiation and true digital signatures can do so by leveraging Entrust IdentityGuard mobile smart credentials.

  The ability to have a digital ID on a mobile device, and use it to sign transactions, is key to many wholesale applications. Regardless of the channel, mobile or online, mobile smart credentials may be leveraged to provide digital signatures for any transaction.

- **Certificates on Devices.** By deploying digital certificates directly to a user's mobile device, organizations are better able to authenticate the device during any online transaction.

  In cases where wholesale-banking applications are leveraging mobile authentication, this extra assurance helps financial institutions ensure only authorized mobile devices are used for authentication.

A MULTILAYERED APPROACH

More than just a simple mobile application, Entrust solutions secure all facets where mobile devices interact, connect and communicate with a financial institution's or corporation's environment. Whether by placing digital certificates directly on user smartphones or by leveraging one of the many options afforded by Entrust IdentityGuard, Entrust helps organizations embrace the ubiquity of mobile devices within any given environment.

Multiple Identities, One Device
Embrace the power of mobile efficiency by enabling multiple digital identities on a single device. This provides independent activation and control, plus customization that ensures brand integrity remains intact.

Soft Tokens & Transaction Notification
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. Transaction notifications help users confirm online transactions, as well as help FIs fight man-in-the-browser malware in the consumer space.

Popular Platforms
Entrust IdentityGuard 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, Google Android, RIM BlackBerry and Microsoft Windows Mobile (6.0-6.5).

Easy Integration
Entrust's open API architecture allows for tight integration with today's leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors. This enables Entrust IdentityGuard to work with new and existing enterprise implementations, plus adds the ability to integrate in-house or managed service-based digital certificates.

For Developers
Entrust's easy-to-use software development kits (SDK) help organizations create customized mobile authentication applications tailored to the requirements of a specific environment. Entrust's authentication capabilities can be embedded transparently into existing mobile applications, further simplifying security on mobile devices for the end-user.

Secured by the Certificate
With Entrust's simple on-boarding of digital certificates, organizations may leverage the power of certificate-based authentication for applications, VPNs, wireless networks and more.

For organizations that have implemented certificate-based security (e.g., for VPN access, authentication, signing and encryption) many are experiencing technical challenges in enrolling and managing certificates on new mobile devices. Entrust provides consistent and clear methods to enroll and manage certificates on mobile devices devices.

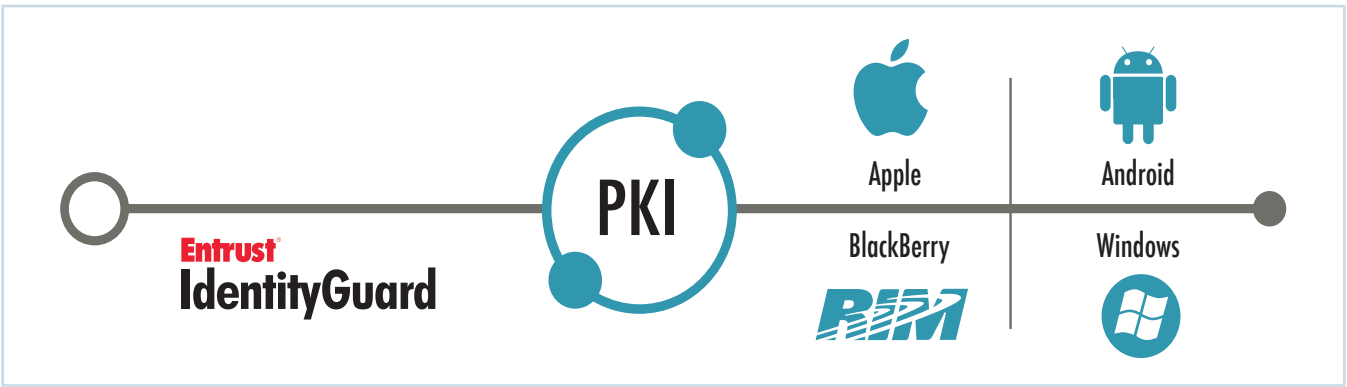

Figure 2: Entrust IdentityGuard issues and manages digital certificates for today's most popular mobile platforms.

SECURITY ON

A MOBILE REALITY WITHIN THE ENTERPRISE

Today, comprehensive versatile authentication platforms are able to capitalize on the proliferation of mobile devices for better enterprise security. Mobile devices can be leveraged as very flexible, convenient and low-cost methods for authentication. By deploying soft tokens or digital certificates to a mobile device, organizations can dramatically reduce obstacles that once made traditional enterprise-wide deployment of physical one-time-passcode (OTP) tokens impractical.

Better Enterprise Security

Much like the approach to securing mobile-banking customers, affordable solutions are available to secure mobile devices that interact or gain access to corporate environments. And these same devices can be transformed into low-cost, easy-to-use authenticators of employee and staff identities.

- **Platform-Based Authentication.** Mobile employees aren't the only users who require proper authentication. Each and every enterprise identity and device needs to be vetted, authorized and managed. By deploying a comprehensive software authentication platform, these tasks can be greatly simplified by one solution — from a single, trusted security expert.

- **Simple Soft Tokens.** Enterprises can deploy soft tokens to any smartphone or mobile device to help authenticate user identities when connecting to corporate networks, applications or resources.

- **Managing Mobile Certificates.** Digital certificates are one of the most effective ways to identify and authenticate electronic entities. Used globally in a myriad of security applications, this trusted technology authenticates mobile devices that require access to corporate information and networks.

  Unfortunately, the complexity of deploying and managing certificates deters many organizations from utilizing certificate-based security on mobile devices — exposing organizations to IT security threats due to weak identity and authentication methods.

- **Mobile Smart Credentials.** Entrust provides true enterprise-grade authentication by leveraging mobile devices and today's advanced communication standards.

  The Entrust IdentityGuard software authentication platform enables smart credential capabilities on mobile devices for physical and logical access, but also provides smartcard-based security for desktops and laptops without native smartcard readers or drivers.

  Organizations may also capitalize on advanced near-field communication (NFC) and Bluetooth standards for more convenient physical and logical access authentication.

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

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. © 2012 Entrust. All rights reserved.

24317/5-12