

Mobile Security Solutions

Securing & Leveraging the Mobile Enterprise

The proliferation of mobile devices is front and center for virtually all organizations, in both employee and customer communities.

Within the enterprise, mobile helps streamline business processes, increasing responsiveness and efficiency. In contrast, mobile also presents tremendous opportunities to engage customers and provide new and differentiated services.

Whether it's for banking, online services or Web-based transactions, this shift has forced financial institutions, e-commerce companies and any organization with an online presence to re-think how they service customers — particularly from the mobile channel.

The Mobility Challenge

As the use of mobile devices and applications grows — and bring-your-own-device (BYOD) initiatives become more commonplace — so do the security risks and attacks targeting user identities, intellectual property, customer data and financial assets.

Organizations are challenged with properly authenticating both employee-owned and company-issued mobile devices connecting to networks, as well securing mobile applications that access corporate systems, data and customer accounts.

And while rolling out mobile applications to customers offers business advantages, it also opens the risk aperture as customers conduct sensitive transactions on smartphones that may be compromised.

The Opportunity: Embrace the Mobile Movement

To effectively mitigate risk, enable true efficiency and satisfy customers in the mobile environment, organizations must properly **secure** mobile devices — but in a way that minimizes user barrier and frustrations. Once secured, organizations then have the opportunity to **leverage** mobile devices to actually improve security in other parts of the business.

For the Enterprise

In the enterprise, secured mobile devices are effective, popular and may be leveraged as a virtual employee identity to securely access computers, applications, cloud services and even physical doors. In high-risk situations, mobile may be leveraged to provide identity-assured transactions that effectively defeat malware-based attacks.

For the Financial Customer

In contrast, smartphones may be used to empower customers to better secure online transactions and defeat malicious fraud attacks that attempt to hijack customer accounts. This movement holds the promise of safe, convenient and always-in-hand solutions to secure identities and transactions across various environments.

This two-pronged approach — first **secure** the device, then **leverage** it to improve security — is an effective method to reduce business risk and introduce new, innovative transactional services that improve the user experience for customers and employees. It's a true differentiator in an already competitive marketplace.

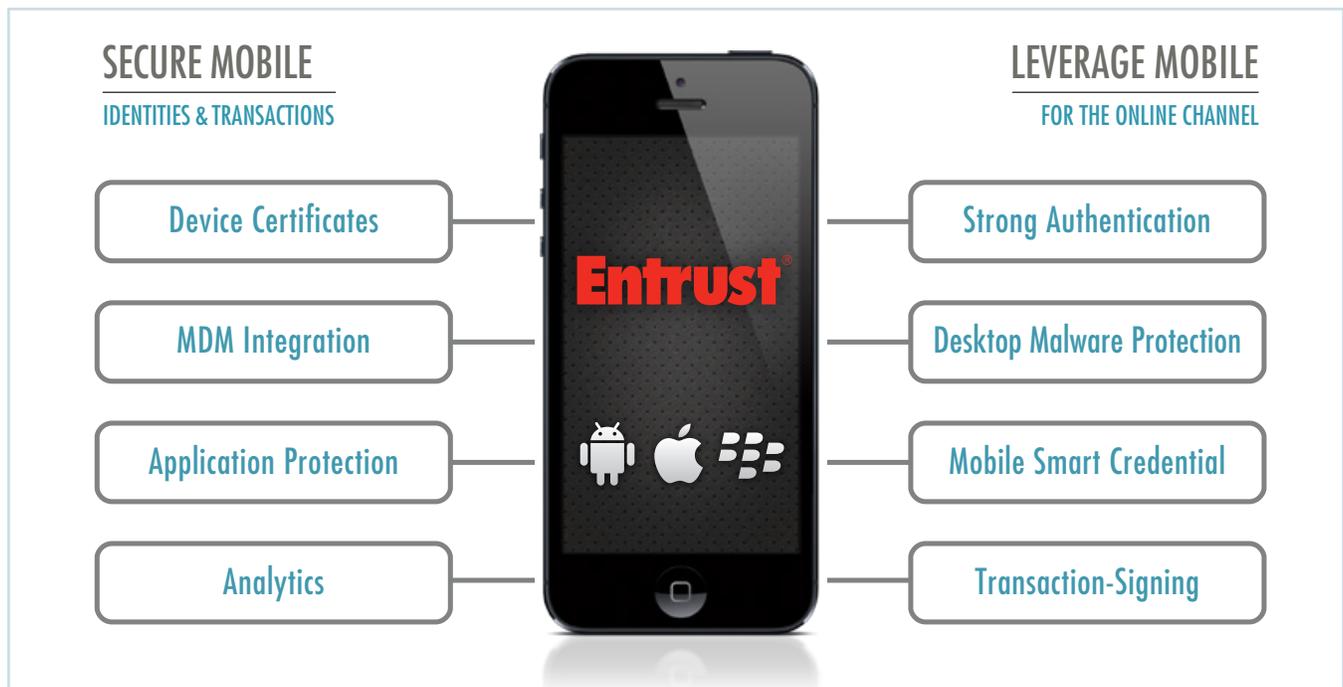
Solution Benefits

- Serves as a comprehensive solution that addresses all your mobile needs
- Reduces business risk and introduce innovative mobile-based services for customers and employees
- Secures mobile devices, applications and transactions
- Defeats the most advanced fraud threats with identity-assured transactions that enhance your mobile brand
- Roll out mobile-based services that leverage mobile identities to improve business efficiency and client interactions
- Use flexible deployment options to meet specific needs
- Deployed as an integral element of Entrust IdentityGuard to address the identity security needs of today and tomorrow

 entrust.com/mobile

SECURE MOBILE, LEVERAGE MOBILE

Entrust offers a number of capabilities that not only help secure mobile identities and transactions, but also empower organizations to leverage mobile devices to improve overall security and streamline business processes. Security controls are increased across all channels, enabling more convenience for employees and customers alike.



SECURE MOBILE IDENTITIES & TRANSACTIONS

With the huge dependence on mobile to execute business operations, organizations are provisioning solutions that not only address security needs, but also ensure the mobile experience is simple and unencumbered.

Entrust solutions authenticate mobile devices connecting to a network, encrypt and digitally sign mobile email communication, embed identity protection into mobile applications, and monitor transactions to detect fraudulent or unauthorized activity. Entrust also offers a range of on-premise, hosted and pre-integrated mobile device management (MDM) capabilities to suit your needs.

Device Certificates

USE CASE >>> Enterprise Mobility & BYOD

Verify who's connecting to networks by provisioning mobile-based digital certificates to secure access to corporate Wi-Fi and VPNs, and encrypt mobile email communication. Device certificates may be distributed via a number of convenient methods, including Entrust IdentityGuard Cloud, to help enable strong mobile security and ensure compliance.

MDM Integration

USE CASE >>> Enterprise Mobility & MDM

Extend the value of digital certificates with automatic certificate provisioning via established MDM policy. Leverage Entrust's rich API suite or pre-built integration with the top MDM vendors, including AirWatch, MobileIron and Good Technology, to combine the benefits of MDM with strong device identities.

Application Protection

USE CASE >>> Mobile Applications for Customer & Enterprise Environments

Leverage Entrust's software development kits (SDK) to embed certificate-based or transparent one-time passcode (OTP) security right into mobile applications. This strong user authentication is transparent to the end-user (i.e., no more passwords), helps defend against distributed denial of service (DDOS) attacks and restricts access to trusted mobile applications.

Analytics

USE CASE >>> Monitor Mobile Transactions for High-Risk or Suspicious Activity

Use real-time monitoring and intervention to identify and stop suspicious or high-risk transactions that stem from both the mobile and online channels. Entrust builds user behavior profiles that may be used to protect mobile transactions, such as money transfers, payments, stock trades or even changes in account information.

LEVERAGE MOBILE FOR THE ONLINE CHANNEL

Using mobile devices for strong authentication and identity-assured transactions is the secure, practical and cost-effective approach to enable organizations to unlock the power of mobile computing. Entrust offers a number of solutions to defeat malware and secure access to logical, cloud and physical resources.

Strong Authentication

USE CASE >>> Online Access to Customer & Enterprise Applications

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. Eliminate the cost and complexity of hard tokens with secure, over-the-air (OTA) provisioning to mobile end-points.

Desktop Malware Protection

USE CASE >>> Commercial Banking > Enterprise Fraud Threats

Stop fraud attacks that target critical assets such as online banking, e-commerce, cloud services and even employee desktops. Identity-assured transactions stop desktop malware and session-riding attacks, securing the enterprise and customer data. Leverage mobile applications to confirm transactions on channels that are far more secure and simple to use than basic approaches such as SMS. In addition, leverage transaction verification to offer easy-to-use, anywhere, anytime dual-control services.

Mobile Smart Credential

USE CASE >>> Mobile Enterprise Credentials for Physical, Logical & Cloud Access

Eliminate hard tokens, passwords and physical access cards with an always-on-hand smartphone. Embed smart credentials on employee smartphones to create trusted identity credentials for stronger, more convenient enterprise authentication. Mobile smart credentials use near-field communication (NFC) or Bluetooth standards to securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data.

Transaction-Signing

USE CASE >>> Commercial & Retail Banking > Enterprise Workflow Efficiency

Deploy mobile-based smart credentials to implement qualified digital signatures to legally authorize transactions, increase efficiency and enable new business services in both enterprise and customers processes. With mobile-based digital signing built into mobile applications, organizations eliminate the need for complex client-side software and expensive signing tokens — all while delighting customers with new, convenient services.

MORE FLEXIBILITY, MORE CONTROL

Popular Platforms

Entrust's mobile solutions are available on today's leading mobile platforms, including Apple iOS, Google Android and BlackBerry.

Your Brand, Our SDKs

Entrust's easy-to-use software development kits (SDK) help organizations create customized or branded mobile authentication applications tailored to the requirements of a specific environment. Entrust's authentication capabilities may be embedded transparently into existing mobile applications, further simplifying both security and the user experience.

Multiple Identities, One Device

Embrace the power of mobile efficiency by enabling multiple digital identities on a single device or even distinct identities sharing a device. This provides independent activation and control, plus customization that ensures brand integrity remains intact.

Critical Security, Convenient Controls

Entrust mobile security solutions are available in two core identity formats, including digital certificates or OATH-based OTP controls, and provide organizations with the flexibility in addressing evolving business needs.

Embed forced-PIN control to protect access to mobile applications or implement policies to detect when a user device has been jailbroken, which could lead to a critical void in security.

Entrust also supports a rich suite of over-the-air provisioning and user self-service capabilities that can be integrated into onboarding and distribution processes.

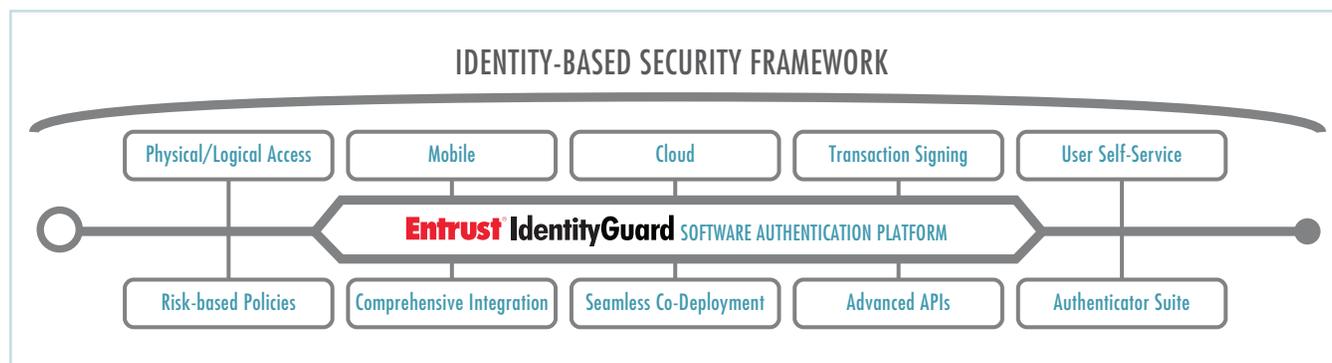


SECURITY
ON

THE TRUE IDENTITY PLATFORM

Entrust's mobile security solutions are an integral element of the Entrust IdentityGuard software authentication platform — an enterprise-wide solution that solves the identity challenge once and for all.

Whether by placing smart credentials 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.



Any Authenticator, One Platform

Entrust's diverse set of authentication capabilities include smartcards and USB tokens, soft tokens, grid cards and eGrids, IP-geolocation, questions and answers, mobile smart credentials, out-of-band OTPs (delivered via voice, SMS or email), out-of-band transaction verification and a range of one-time-passcode tokens.

Mobile Self-Help

Via the secure, Web-based Entrust IdentityGuard Self-Service Module, end-users may manage many aspects of their accounts — device enrollment, obtaining certificates, provisioning and more — freeing administrator time without compromising the security of the network.

Rich APIs & Application 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.

Identities from the Cloud

With Entrust IdentityGuard Cloud, organizations may seamlessly provision and manage digital certificates and identities — for both users and mobile devices — without standing up their own certificate infrastructure. This approach reduces costs, increases efficiency, and simplifies setup and deployment.

Future-Proofed

Be ready for what's next. Entrust's versatile platform approach enables organizations to introduce or change mobile security controls — camera, voice channel, GPS or touch patterns, for example — with little or no adverse effects on the environment or user population.

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 secures 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