

Entrust IdentityGuard Mobile Smart Credential

Transforming Mobile Devices into Multipurpose Digital Identities

Targeted cyberattacks, fraud schemes and legislated regulatory mandates continue to grow in scope and sophistication while both employees and customers have increased expectations for more convenient, simple-to-use security.

Not only are traditional security controls ineffective in defeating advanced threats, but provisioning costs and complexity are increasing.

In response, organizations are ready to leverage the power and convenience of mobile devices as easy-to-use authenticators for both internal employees accessing physical and logical resources, and customers accessing mobile and online services.

The Transformation: Mobile Device to Digital Identity

The Entrust IdentityGuard Mobile Smart Credential is an innovative mobile application that transforms a mobile device into a virtual smartcard, eliminating the need for plastic smartcards, one-time-passcode hardware tokens and even passwords.

Compared to traditional approaches, the Mobile Smart Credential is more convenient, easier to use, cost-effective to deploy and provides support for a number of authentication and information-protection needs within the enterprise and across customer bases.

Simple User Experience for Customers & Employees

Deploying strong authentication credentials on employee and customer mobile devices not only meets security needs, but dramatically simplifies the end-user experience with ease and convenience.

Identity credentials will always be on hand — no more single-purpose smartcards, OTP tokens, complex passwords or costly resets. Entrust IdentityGuard supports rich policy and workflow engines that simplify credential issuance and temporary replacement or recovery, requiring fewer demands on IT help desks.

The Entrust IdentityGuard Mobile Smart Credential provides the best line of defense against malware-based attacks (e.g., man-in-the-browser) and opens the door for streamlining business processes with anywhere, anytime mobile digital signatures.

Product Benefits

- Transform mobile devices into virtual credentials for secure access to networks, applications and physical resources
- Leverage mobile for out-of-band transaction confirmation to defeat desktop-based malware
- Streamline business services with anywhere, anytime mobile digital signatures
- Extend strong identities for secure cloud access, encryption and digital signatures
- Reduce total cost of ownership by removing need for expensive physical form factors, printers and specialty desktop readers
- Future-proof authentication investments with platform approach that easily integrates with new security technology

Diverse Enterprise Use Cases

- Secure logical access, including Windows Smartcard Logon, VPN and cloud-based applications
- Secure physical access to facilities
- Digital-signing of desktop forms, documents and emails
- Encryption of desktop email and information

MULTIPLE IDENTITIES, ONE DEVICE

In certain situations, users may require support for multiple identities. With the Mobile Smart Credential, multiple identities may be stored in one smart credential identity container, eliminating the need for multiple smartcards and access credentials.

Defeat Malware Attacks on Customer & Enterprise Accounts

From securing corporate bank accounts to verifying business transactions, leverage mobile devices to review and approve critical transactions on a separate, secure channel.

Identity-assured transactions are a proven defense against malware, advanced persistent threats and other online fraud. Move transactions out-of-band to the mobile channel to review exact transaction details, and also provide real-time confirmation and approval from the convenience of a smartphone.

The Entrust IdentityGuard Mobile Smart Credential is an effective and elegant method to strongly secure digital identities, but also is used to safely authenticate Web or cloud transactions to defeat advanced malware and other nefarious attacks.



Streamline Business with Mobile Digital Signatures

Internal business processes and customer-facing services often require legally binding digital signatures that are fundamental for day-to-day operations. But traditional methods are cumbersome, slow and fail to drive business.

Entrust IdentityGuard Mobile Smart Credentials help organizations streamline business with strong, non-repudiated digital signatures — right from a mobile device.

Any document or transaction that requires formal approval may be executed right from today's most popular smartphones. The end-user's secure, authenticated digital identity is used to create a digital signature that is both legally binding and provides trusted non-repudiated.

REDUCE COST & COMPLEXITY

With ongoing pressure to reduce IT capital expenditure and operating expense, the Entrust IdentityGuard Mobile Smart Credential solution helps eliminate the need for physical smartcards, card-printing and personalization systems, as well as the complex IT processes to enroll and provision user accounts.

The solution leverages the power of mobile computing and over-the-air (OTA) provisioning, as well as rich policy and workflow capabilities, to eliminate manual processes and empower end-users to easily enroll and recover credentials as required.

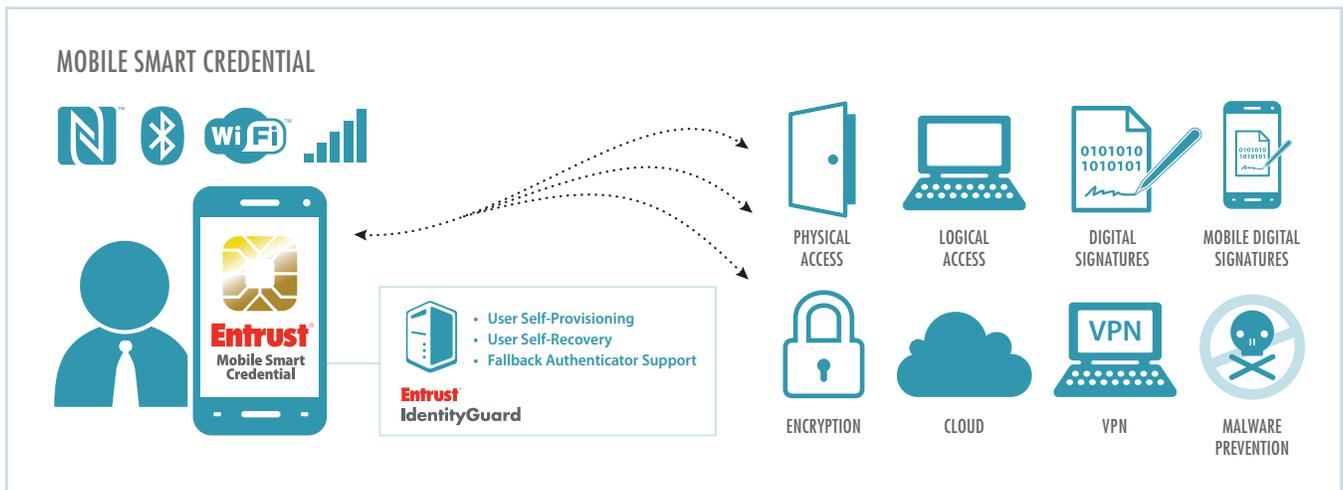


Figure 1: The Entrust IdentityGuard Mobile Smart Credential helps organizations leverage mobile devices to reduce overall cost, defeat malware, implement mobile-based digital signatures and simplify secure physical, logical and cloud access.



SOLUTION ADVANTAGES

Entrust provides organizations a comprehensive solution that consolidates certificate and identity management, as well as all respective authentication requirements, within a single platform. By leveraging Mobile Smart Credentials, organizations are able to reduce cost and complexity, future-proof investment and integrate advanced technology for greater security.

Future-Proof Solution

Maximize your authentication investment by ensuring it's flexible enough to leverage future security technology to help adapt to the next evolution of attacks.

The framework extends identities to physical access, cloud-based applications and new authentication approaches as the technology, threat landscape and business needs evolve.

Defeat Malware

Mobile devices provide a separate channel from user desktops and may be leveraged for out-of-band transaction verification to defeat malware-based threats such as man-in-the-browser and other malicious attacks (e.g., Trojan variations).

Deploy New Customer-Facing Services

Deploying identities on mobile devices provides a number of business opportunities to eliminate cumbersome and costly paper-based processes for formal approvals.

Mobile digital signatures speed the pace of business and deliver convenient methods for employees and customers to provide approval or verification of transactions, communication and other sensitive information.

NFC & Bluetooth Integration

Taking advantage of near-field communication (NFC) and Bluetooth standards, Entrust embeds biometrics and digital certificates on smartphones to create trusted identity credentials for stronger, more convenient enterprise authentication. Authenticated desktop logins are as simple as having a mobile device in proximity of a workstation.

Automatic Credential Detection

Remove the human element by leveraging Entrust's automatic workstation logout features, which engage when an end-user leaves the premise, desk or work area.

With Bluetooth and NFC integration, the solution automatically detects mobile devices with embedded credentials. The solution asks the user to enter their PIN when they approach their workstation, removing the outdated need to enter usernames and passwords.

Proximity-Based Logout

Entrust offers proximity-based automatic logout that helps increase security — a critical capability for organizations that require shared workstations (e.g., doctors, stock traders).

Reduce TCO, Simplify Credential Provisioning

By eliminating the need to issue and deliver physical authenticators and desktop smartcard readers, provisioning efforts, cost and daily management are greatly reduced. The solution provides simple over-the-air provisioning (OTA) and helps streamline user enrollment and self-recovery.

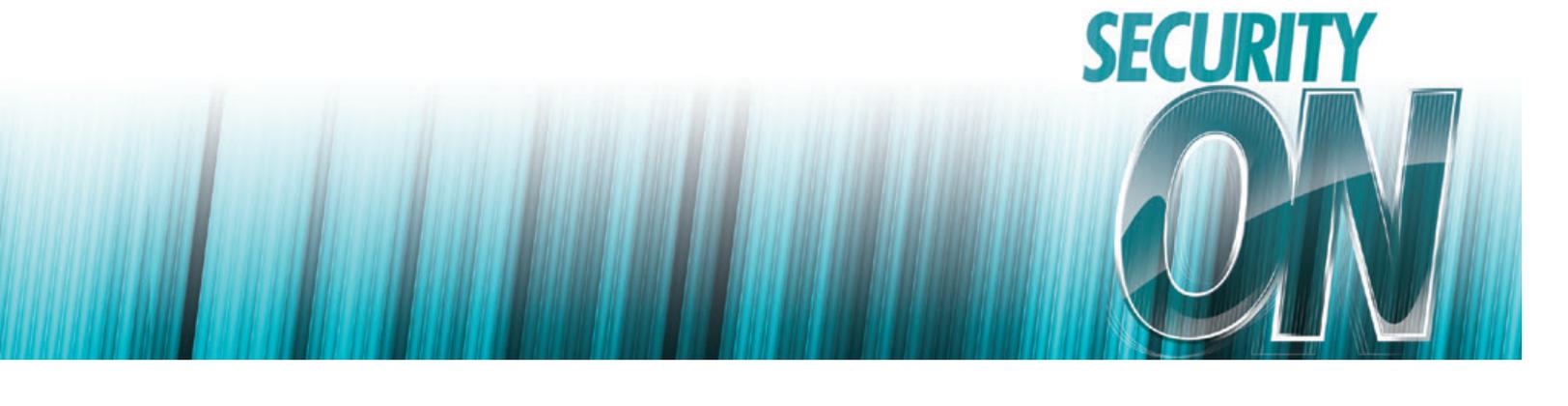
Broad Platform Support

Supports the leading mobile platforms on the market today, including Apple iOS, BlackBerry and Google Android.

Authentication Policies

Entrust's framework provides support for varied authentication policies across different user communities (e.g., internal departments, customers or partners) and gives the ability to change a user's authenticator with minimal cost or effort should business needs or security threats dictate.

The approach empowers organizations to dynamically evolve to address advanced identity threats in real time.



SECURITY
ON

ENTERPRISE-WIDE AUTHENTICATION PLATFORM

Entrust's comprehensive platform serves as an organization's single identity-based security solution to bridge emerging technologies for strong mobile, cloud and smart credentialing offerings. Underpinned with rich policy engines and broad deployment options, Entrust solutions strengthen security, maximize staff efficiency and reduce overall costs.

- Solve authentication, once and for all, across the enterprise
- Provide agility to adapt to change in real time
- Rich options for deployment flexibility
- Future-proof to protect investment and grow as needs evolve

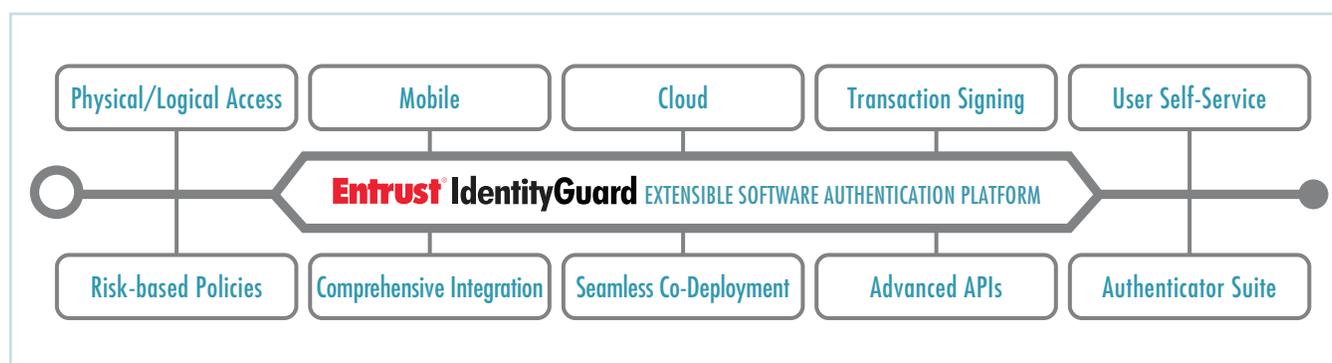


Figure 2: Entrust IdentityGuard Mobile Smart Credentials are a critical component of Entrust's comprehensive security framework.

ENTRUST & YOU

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service.

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

Company Facts

Website: www.entrust.com
 Employees: 359
 Customers: 5,000
 Offices: 10 globally

Headquarters

Three Lincoln Centre
 5430 LBJ Freeway, Suite 1250
 Dallas, TX 75240 USA

Sales

North America: 1-888-690-2424
 EMEA: +44 (0) 118 953 3000
 Email: 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