Entrust Datacard™

Entrust IdentityGuard Mobile Smart Credential

Transform Mobile Devices into Multipurpose Digital Identities

Even the best IT organizations experience difficulty managing the sheer volume of identities within their organization. It's no longer sufficient to manage just desktops, as the infrastructure has moved well beyond static environments. Mobile devices are now the platform of choice.

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

Mobile Device to Digital Identity

These multipurpose credentials securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data. It's 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.

▶ entrust.com/mobile

Simple User Experience

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.

Efficiency from the Cloud

Entrust IdentityGuard Mobile Smart Credential can be managed either on-premise or via the cloud. Both management infrastructures improve efficiency and accelerate ROI by providing a secure and scalable consolidated digital identity. If accessed from our Entrust Certificate Services™ management platform, Entrust IdentityGuard Mobile Smart Credential can be integrated with other digital security applications which eases the burden of managing security and allows staff and resources to focus on their core business and responsibilities.

▶ entrust.com/CloudPKI

Multipurpose Credentials

Gain 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. Rich policy and workflow engines simplify credential issuance and temporary replacement or recovery, requiring fewer demands on IT help desks.

+1-888-690-2424

entrust@entrust.com
entrust.com/mobile-credentials

@EntrustDatacard
+entrust
/EntrustVideo
/EntrustSecurity

Service Benefits

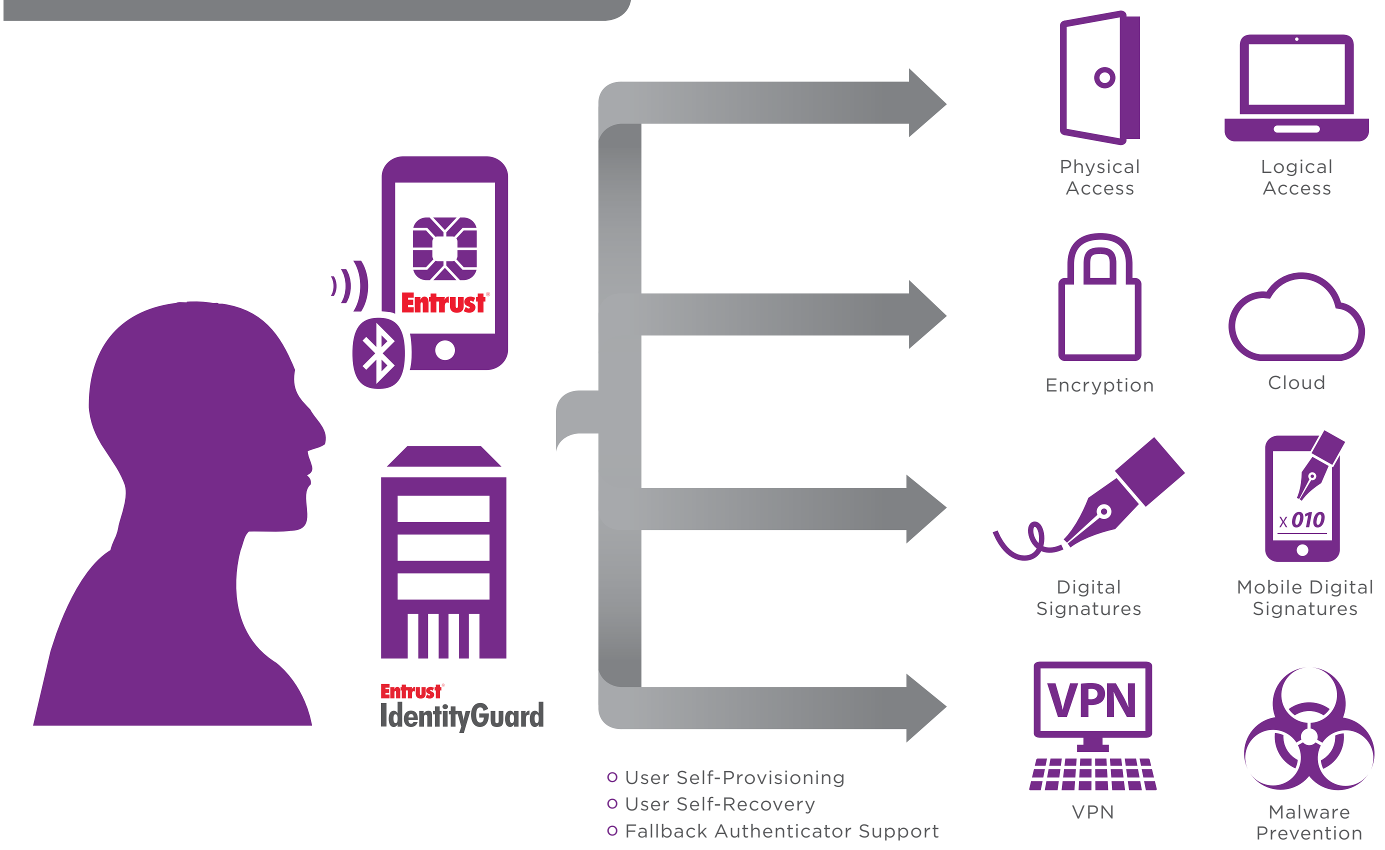
- Key component of the Entrust IdentityGuard solution
- Transform mobile devices into virtual credentials for secure access to networks, applications and physical resources
- Leverage mobile for out-of-band transaction confirmation to defeat desktop-based malware
- Streamline business services with anywhere, 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
- Developed for the real world with out-of-the-box support for iOS, Android and BlackBerry mobile operating systems

Reduce Cost & Complexity

With ongoing pressure to reduce IT capital expenditure and operating expense, the 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.

Entrust IdentityGuard Mobile Smart Credential



The always-on-hand credential. Leverage mobile devices to reduce overall cost, defeat malware, implement mobile-based digital signatures and simplify secure physical, logical and cloud access.

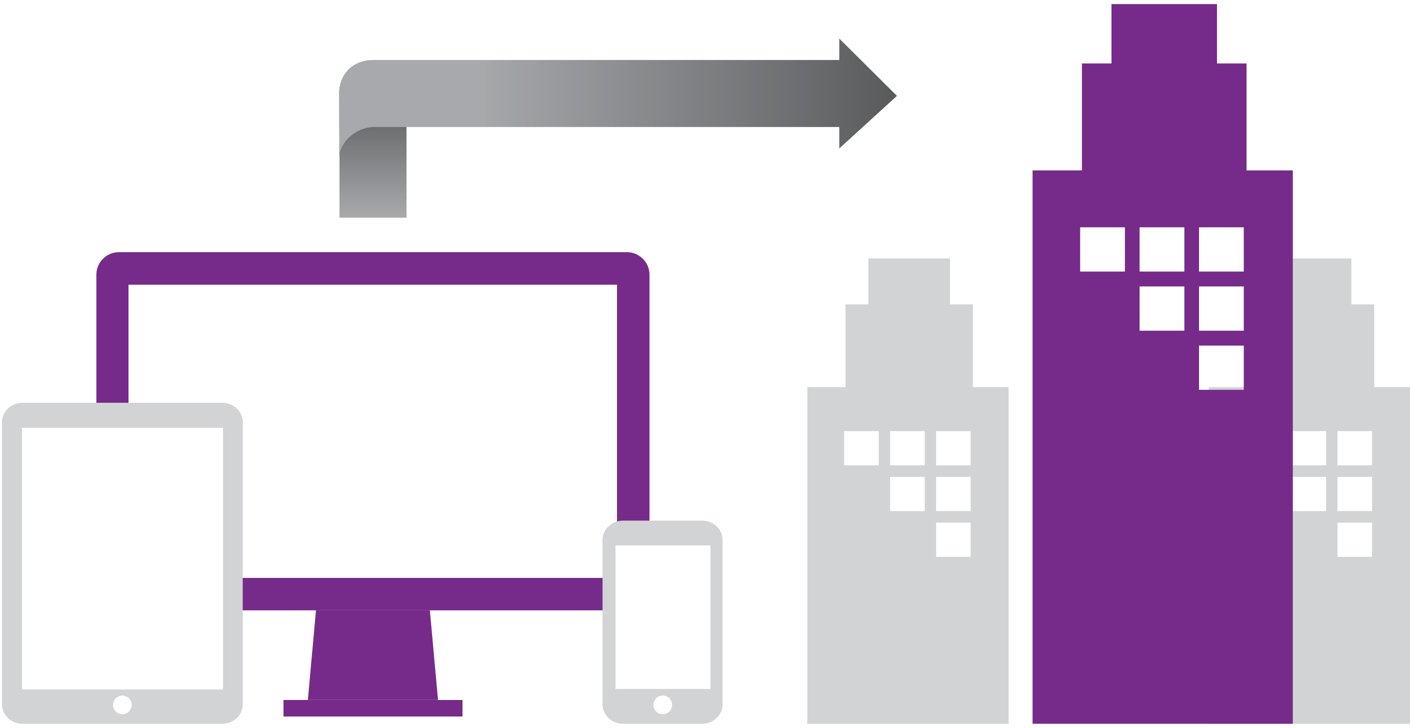
Flexible Integration

Developed for use in the real world, the Mobile Smart Credential supports today's most popular mobile platforms, including Apple iOS, Google Android, and BlackBerry.

The solution offers built-in integration for simple deployment, regardless of the mobile operating systems used within your environment. This flexibility enables IT organizations to work with end-users and provides a means of a true bring-your-own-device (BYOD) service while still enabling controlled service.

Diverse Enterprise Use Cases

- Secure logical access, including Microsoft® 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.

Secure Customer & Enterprise Accounts

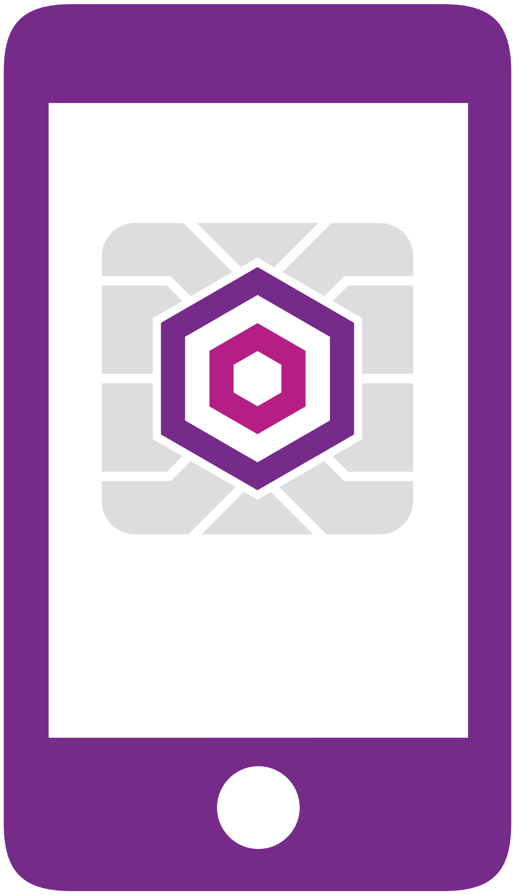
From securing corporate bank accounts to verifying business transactions, leverage mobile devices to review and approve critical transactions on a separate, secure channel.

Defeat Malware & APTs

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.

Authenticate Web & Cloud Transactions

The 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.



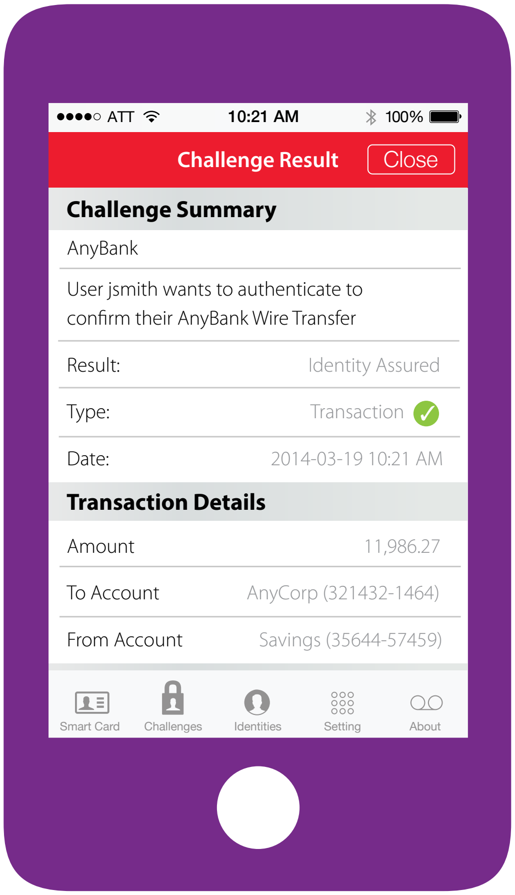
Mobile Digital Signatures Streamline Business

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.

The Mobile Smart Credential helps organizations streamline business with strong, non-repudiated digital signatures — right from a mobile device.

Create Legally Binding Digital Signatures

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.



Challenge Summary

AnyBank

User jsmith wants to authenticate to confirm their AnyBank Wire Transfer

Result:	Identity Assured
Type:	Transaction ✓
Date:	2014-03-19 10:21 AM

Transaction Details

Amount	11,986.27
To Account	AnyCorp (321432-1464)
From Account	Savings (35644-57459)

Banking verified. Mobile out-of-band transaction verification enables users to raise a concern about potential fraud or confirm the legitimacy of transactions.

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.

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.

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.

Business Made Efficient

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.

Solution Advantages (continued)

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.

Defeat Advanced Malware

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. 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).

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.

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).

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™