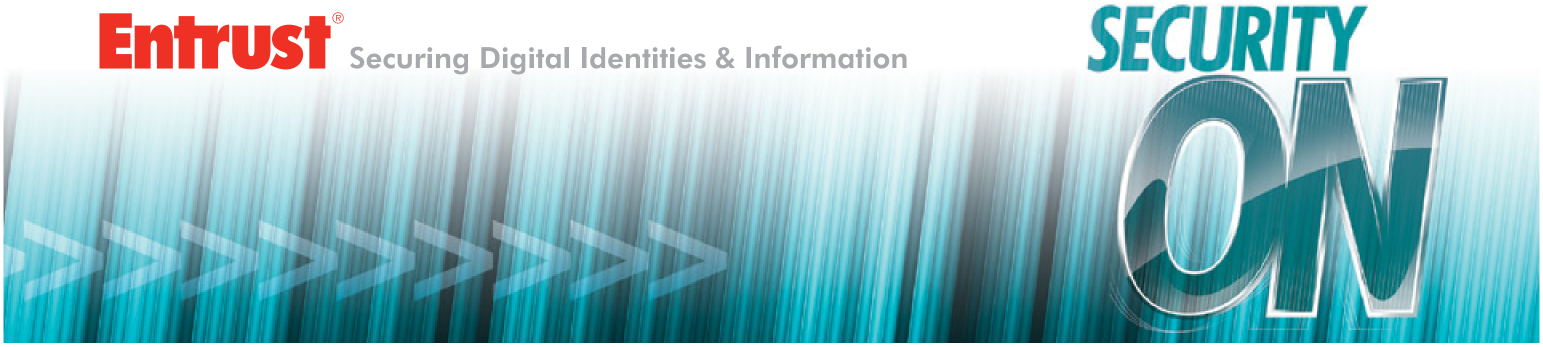
Entrust® Securing Digital Identities & Information



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, driving the need to strengthen security while concurrently reducing costs.

While traditional smartcards provide effective security controls, they are not without their own challenges. Costs of smartcard replacements, card-printing workflows and encoding, as well as the need for ongoing operational support, are objections often raised by IT departments.

In response, organizations are ready to leverage the power and convenience of mobile devices as easy-to-use authenticators for physical and logical access, possibly as a core component of a bring-your-own-device (BYOD) strategy.

This clearly sets the stage for new innovation that meets security, usability and cost considerations.

The Transformation — Mobile Device to Mobile Smartcard

Entrust IdentityGuard Mobile Smart Credential is an innovative mobile application that transforms a mobile device into a virtual smartcard, eliminating the need for physical smartcards or hardware-based one-time passcodes (OTP).

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 an organization.

Simple User Experience

Deploying strong authentication credentials on employee 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.

Support for Multiple Identities

In certain situations, employees 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.

Entrust's Mobile Smart Credentials may be leveraged to solve a wide array of use-cases:

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

Product Benefits

- Address regulatory compliance and privileged access security needs with lower cost and complexity
- Transform mobile devices into working smartcard credentials for secure physical and logical access
- Enable enterprises to capitalize on BYOD initiatives to improve identity-based security with features such as proximity-based login/logout
- Extend strong identities for secure cloud access, encryption and digital signatures
- Increase security with automatic session logout and improve convenience with proximity detection
- Reduce total cost of ownership by removing need for expensive physical form factors, printers and specialty desktop readers
- Future-proof authentication investments with a platform approach that easily integrates with new security technology
- Increase adoption by supporting leading mobile platforms including Apple iOS, RIM BlackBerry and Google Android

REDUCE COST & COMPLEXITY

With ongoing pressure to reduce IT capital expenditure and operating expense, Entrust's 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, as well as rich policy and workflow capabilities, to eliminate manual processes and empower end-users to easily enroll and recover credentials as required.

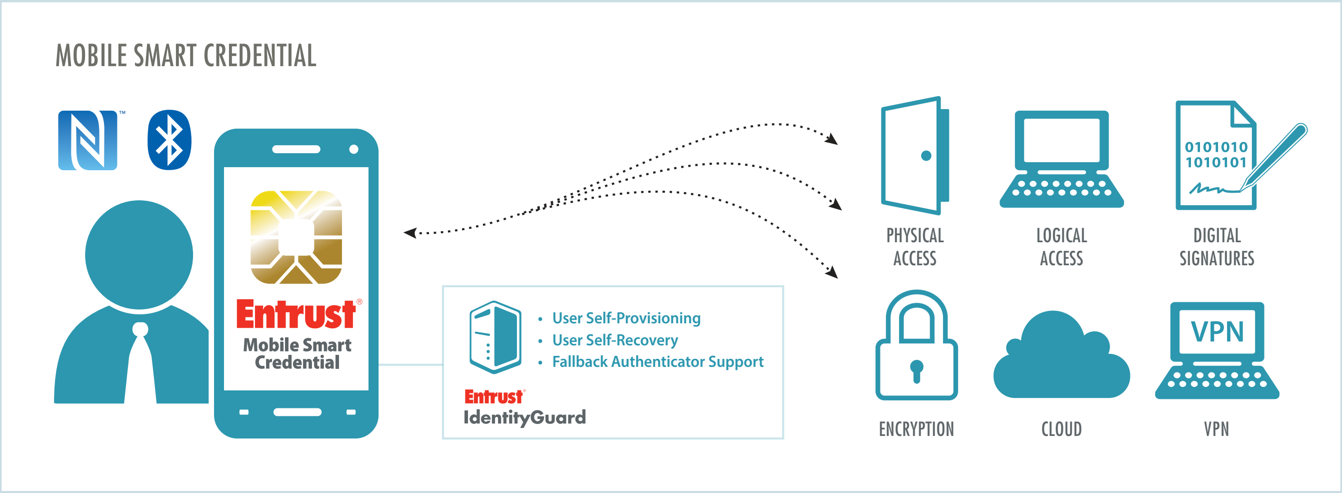


Figure 1: Entrust's Mobile Smart Credential helps organizations leverage bring-your-own-device initiatives to reduce overall cost and simplify secure physical, logical and cloud access.

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.

And because mobile devices provide a separate channel from user desktops, they 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.

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 username and passwords.

Reduce TCO

By eliminating the need to issue and deliver physical authenticators, desktop smartcard readers and costly credentials, provisioning efforts and daily management are greatly reduced. The solution helps remove the high costs associated with physical cards, printers and specialized desktop readers.

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).

Broad Platform Support

Supports the leading mobile platforms on the market today, including Apple iOS, RIM 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. The approach empowers organizations to dynamically evolve to address advanced identity threats in real time.

ENTERPRISE-WIDE FRAMEWORK

Entrust's comprehensive management framework serves as an organization's single software-based security platform that bridges emerging technologies for strong mobile, cloud and smart credentialing offerings. By seamlessly integrating co-deployment measures, federation security, advanced APIs and self-service management tools, Entrust strengthens security, maximizes staff efficiency and reduces overall costs.

The use of an enterprise-wide strong authentication framework not only simplifies deployment, but enables organizations to build a common security policy framework that extends to physical, logical, cloud and mobile identity access management (IAM) — all under a single environment that adapts authentication challenges based on situational risk.

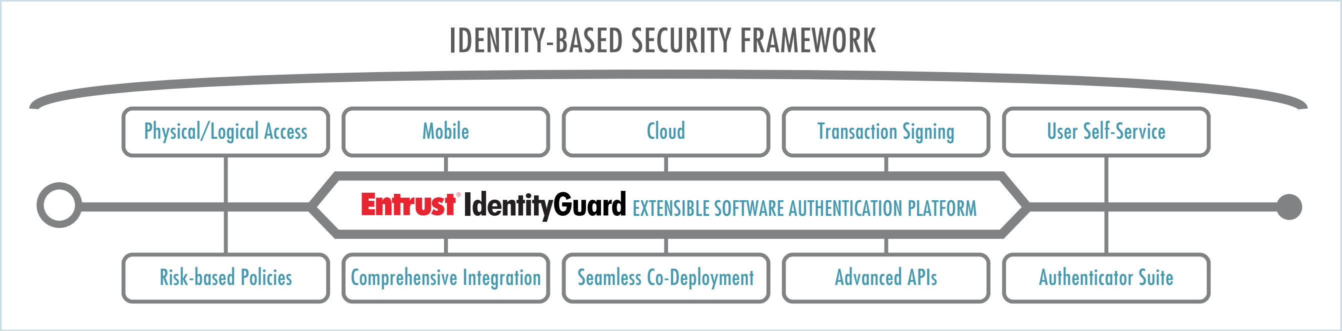


Figure 2: Entrust Mobile Smart Credentials are a critical component of Entrust's comprehensive security framework approach.

Framework Benefits

- Solve authentication, once and for all, across the enterprise
- Provide agility to adapt to change in real time
- Future-proof to protect investment and grow as needs evolve
- Rich options for deployment flexibility
- Extends identities to cloud-based applications
- Secures today's most popular mobile devices
- Provides adaptive, risk-based authentication
- Improves efficiency with seamless integration to card management systems
- Transforms end-user mobile devices into true credential containers

Powered by Entrust IdentityGuard

Entrust's flagship authentication solution, Entrust IdentityGuard, continues to lead the industry as one of the most robust software authentication platforms, delivering an unmatched breadth of capabilities and flexibility to meet the most demanding security environments.

The award-winning Entrust IdentityGuard software authentication platform transforms mobile devices into secure, enterprise-grade credentials for physical and logical access via NFC and Bluetooth communication standards.

Any Authenticator, One Platform

The same Entrust IdentityGuard solution that manages identities or an organization's mobile devices still provides the widest range of authenticators on the market.

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 one-time passcode (delivered via voice, SMS or email), out-of-band transaction verification and a range of one-time-passcode tokens.

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.

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.

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, contact the Entrust representative in your area at **888-690-2424** or visit **entrust.com/authentication.**

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