



Enterprise Authentication

Securing Identities in an Evolving Environment

Today's organization is falling victim to unrelenting attacks that target physical and logical infrastructures, mobile platforms, user identities, network devices and more.

The boundaries of the corporate network are being challenged, as more employees need access wherever they are. Extranets, intranets, Web mail and desktops need strong authentication as they are being accessed from beyond the boundaries of the corporate network.

Couple these threats with the skyrocketing use of mobile devices within an enterprise, plus the need for better convergence between physical and logical access systems, and enterprise security has changed drastically in the last five-plus years.

But by leveraging a cost-effective platform approach, businesses can broaden their security deployment, provide flexibility for employees and partners, while achieving operating efficiencies and maximizing their return on investment.

A New Enterprise Landscape

Mobile or remote employees — the traditional user base for stronger authentication — are commonplace at all levels in all industries. When a limited community of users, with the same basic requirements, needed additional protection, a single authenticator such as tokens (though traditionally expensive and sometimes hard to manage) was a reasonable solution. But that small community of users who need more than password protection has ballooned.

Breaches occur more often, brands are impacted by fraud incidents and important regulations have been implemented to help protect users and information.

While the demand for strong authentication has extended beyond traditional users, technologies now exist that present organizations with new opportunities to improve security, while reducing operating cost. These include physical and logical access solutions, digital certificates on mobile devices, soft tokens, advanced credentialing and more.

Better Authentication Required

Many of the authentication methods and policies from even five years ago are already showing signs of age. As compliance requirements stiffen and attacks become more sophisticated, organizations must remain active in maintaining and evolving advanced security measures and authentication technology.

Simple passwords, even for users operating exclusively internally, are no longer enough to prevent breaches, protect privacy and achieve compliance. Strong authentication must be deployed to a wider audience — efficiently and cost-effectively.

Solution Benefits

- Provides streamlined platform approach for strong authentication, physical and logical access, and mobile authentication — all from a single trusted security expert
- Adjust quickly to changes in the threat landscape, industry regulations or the organization
- Leverage near-field communication (NFC) and Bluetooth standards for more convenient physical and logical access via mobile devices
- Easily add, change or remove authentication functionally as required
- Gain access to widest range of authenticators available via a single platform
- Provides end-to-end capabilities for smartcard selection, issuance and management
- Enables multiple identities to be used on a single mobile device



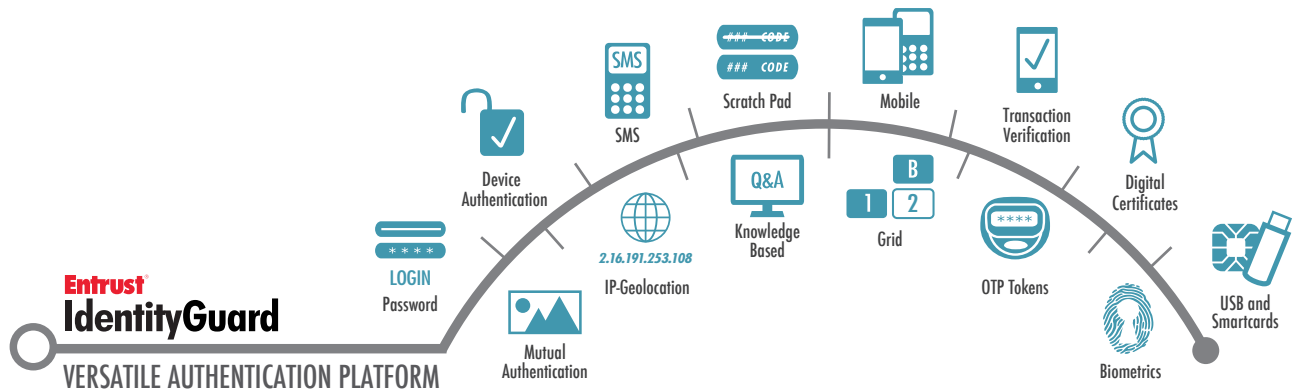


Figure 1: A versatile authentication platform enables organizations to select the right authenticator for each user or device based on risk, cost and access requirements.

Using risk assessment and policy to determine when stronger security is required for access to resources with greater value allows authentication to be layered as needed. And using a platform approach, like the one seen above, offers organizations the ability to select the authentication method based on risk, cost and user access requirements.

Embrace Capabilities of Mobile Devices

Introducing new risks and opportunities for business, mobile devices are used increasingly to access corporate networks. Thus, enterprise authentication strategies must consider how users can strongly authenticate to the network with mobile devices.

At the same time, the proliferation of such devices allows corporations to still employ a single platform 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.

Mobile devices enable organizations to leverage a very flexible, convenient and low-cost method for authentication.

Security via Mobile Devices

- Secure access to corporate resources
- Leverage mobile devices as authenticators
- Use NFC and Bluetooth standards for convenient physical and logical access

Access Convergence

With the evolution of smartcard technology, enterprises can integrate three security environments — physical, logical and mobile access — to provide consolidated management, improved ROI and a total security view. This push toward coupling complete access security not only consolidates efforts, it saves money and reduces the burden on end-users.

Easy for the end-user and more efficient for organizations, this convergence enables everything from credentialing, secure access to facilities, strong authentication to desktops and network resources, and digital signature capabilities — all via a single credential possessed by the end-user on a smartcard, USB or embedded on their mobile device.

And advanced near-field communication (NFC) and Bluetooth capabilities add more convenience for physical and logical access authentication via popular mobile platforms.



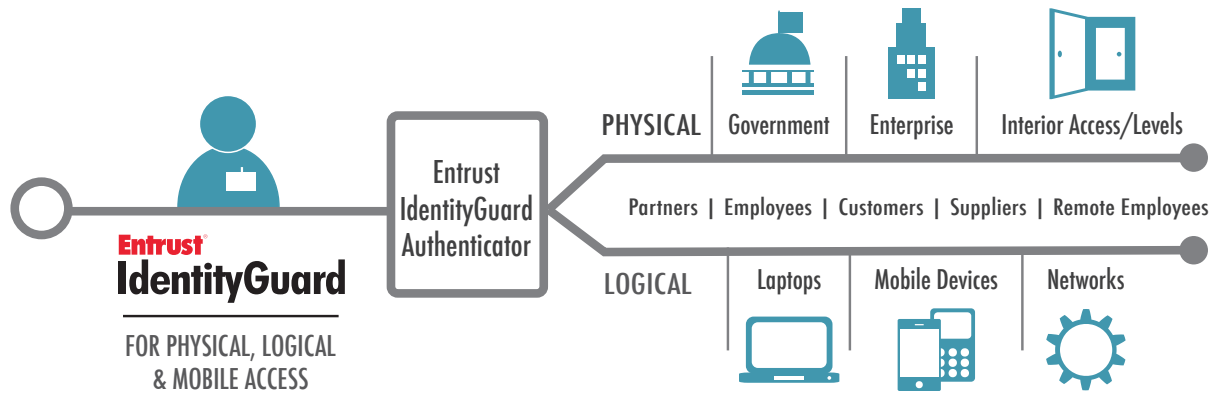


Figure 2: Entrust IdentityGuard leverages smartcards, mobile devices, tokens, digital certificates, biometrics and more to help realize true physical, logical and mobile access convergence in any environment.

Entrust — Identity-Based Security

Unfortunately, existing point authentication solutions are no longer up to the task of thwarting advances that exploit vulnerabilities in a variety of channels or mediums. Whether the root threats originate from internal or external sources, critical information, data and identities are at constant risk.

Organizations need to address authentication requirements of different types of users, provide authentication security over a broad range of access points and ensure they can address new requirements as they evolve. A platform approach provides flexibility and helps meet these requirements cost-effectively.

Strong Authentication

The award-winning Entrust IdentityGuard versatile authentication platform enables organizations to deploy strong authentication throughout the enterprise, enable physical and logical access control, and secure authorized mobile devices co-existing within the infrastructure.

It's important to remember, however, that a one-size-fits-all approach to authentication is not appropriate for most enterprise environments.

Entrust IdentityGuard offers the widest range of authenticators on the market — and all from a single, cost-effective platform. And the addition of smartcards, mobile smart credentials and digital certificates as proven authenticators extends the platform's versatility, scalability and cost-effectiveness.

And as a U.S. Federal government-approved provider of PIV and PIV-I credentials, Entrust is an expert in the Personal Identity Verification (PIV) standards that industries and enterprises are adopting to govern their authentication strategies.

Entrust IdentityGuard

Entrust offers the widest range of authenticators available on the market today — and all from a single platform.

SECURITY
ON

Physical, Logical & Mobile Access

Comprehensive physical, logical and mobile access security is achieved by the use of digital certificates, public key infrastructure (PKI) and a strong authentication platform. This approach enables a single platform to issue and manage digital certificates that are deployed to smartcards, USB or embedded on mobile devices.

As more security measures are implemented, end-users often are burdened with multiple cards, credentials, IDs, badges and tokens. Employees and staff are hindered with locating different credentials, fumbling with "token necklaces" and tracking an unnecessary number of authenticators. Proper convergence helps eliminate this clutter and allows staff to focus on core responsibilities.

A converged security system also allows organizations to reduce the number of vendors, contractors or third parties who are required for separate systems. This equals real cost-savings, enhanced security and a strong return on your investment.

Mobile Security

Whether by placing digital certificates directly on user smartphones or by leveraging one of the many options afforded by Entrust IdentityGuard Mobile, Entrust helps organizations embrace the ubiquity of mobile devices within a given environment.

Entrust provides mobile security capabilities via distinct solution areas — mobile authentication, transaction verification, mobile smart credentials, and transparent authentication technology with an advanced software development kit.

These capabilities are compatible with today's leading smartphone platforms, including the Apple iPhone, Google Android, RIM BlackBerry and Microsoft Windows Mobile (6.0-6.5).

Plus, Entrust's easy-to-use SDK helps 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 enterprise security on mobile devices for the end-user.

Entrust & You

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**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 4,000
Offices: 10 globally

Headquarters

One Lincoln Centre
5400 LBJ Freeway, Suite 1340
Dallas, Texas 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 empowers enterprises, governments, financial institutions, citizens and websites in more than 4,000 organizations spanning 60 countries. Entrust's customer-centric focus is the foundation to delivering organizations an unmatched level of security, trust and value. For strong authentication, credentialing, physical and logical access, mobile security, digital certificates, SSL and PKI, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com. Let's talk.

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. © Copyright 2012 Entrust. All rights reserved.