



## Securing Your Digital Life

### Entrust IdentityGuard for Enterprise

#### Protecting your Enterprise

When an employee or partner accesses the corporate network through an extranet, a remote access gateway (VPN) or through a Microsoft® Windows® desktop, they have effectively opened a door to the corporate network and its data. The security of the network and that of the desktop is only as strong as the way users are authenticated, highlighting the importance of doing this well. Coupled with industry mandates like the Payment Card Industry's (PCI) requirement for protecting sensitive card holder data, organizations are being driven to increase the strength of authentication across a much broader user population than ever before.

The most common way of authenticating employees and partners—username and password—is also one of the weakest forms of authentication used today and has been subject to numerous forms of proven password attacks. Strengthening this type of authentication, through mandating complex long passwords and enforcing frequent changes, often delivers minimal security improvement yet significantly increases help desk costs. Although deployed in small projects—typically remote access—in most organizations, the need to extend strong authentication to a wider audience is increasing. The budgetary challenges highlighted by more widely deploying traditional strong authenticators, such as time-synchronous tokens, is causing organizations to look for a more cost-effective solution that delivers a flexible approach to increasing security without introducing significant costs.

#### Entrust IdentityGuard – A Flexible Strong Authentication Platform

As an established global leader in online security, Entrust has developed an inexpensive strong authentication platform that can help organizations protect the identities of employees and partners accessing sensitive enterprise data. The Entrust IdentityGuard solution allows organizations to layer security across a diverse range of enterprise users, transactions and applications. This enables organizations to apply the right level of strong authentication across the enterprise instead of a select group of users. Entrust IdentityGuard seamlessly integrates with your existing environment with minimal impact on the user experience accessing the network via remote access, the Microsoft Windows desktop, or the extranet. Designed with enterprise security requirements in mind, Entrust IdentityGuard can

#### Product Benefits

- Flexible authentication platform that can be deployed at a fraction of the cost of traditional two-factor options
- Range of authentication methods that can be used across the entire enterprise
- Easy to deploy and manage with a non-invasive architecture



Figure 1: The Authentication Challenge

# Entrust IdentityGuard

provide a broad range of authentication capabilities at a single low price - a fraction of the price of conventional hardware tokens.<sup>1</sup>

## Entrust IdentityGuard Advantages

### Range of Strong Authentication Capabilities.

Entrust IdentityGuard delivers a range of authentication options that can enable stronger authentication across the enterprise without the need to deploy hardware or force significant changes on the user experience. This includes machine, grid-based, knowledge-based or mobile authentication along with mutual authentication to authenticate the web site to the user. Organizations can choose how they want their users to authenticate depending on user type and the application being used, including remote access, Windows desktop and applications deployed on the extranet.

Entrust IdentityGuard can be readily extended to other delivery channels, including Interactive Voice Response and help desk systems. Its authentication methods do not require specialized hardware or direct hardware connections with the computer so it can be leveraged across multiple platforms and used in conducting various types of transactions.

<sup>1</sup> [www.entrust.com/identityguard/calculator](http://www.entrust.com/identityguard/calculator)

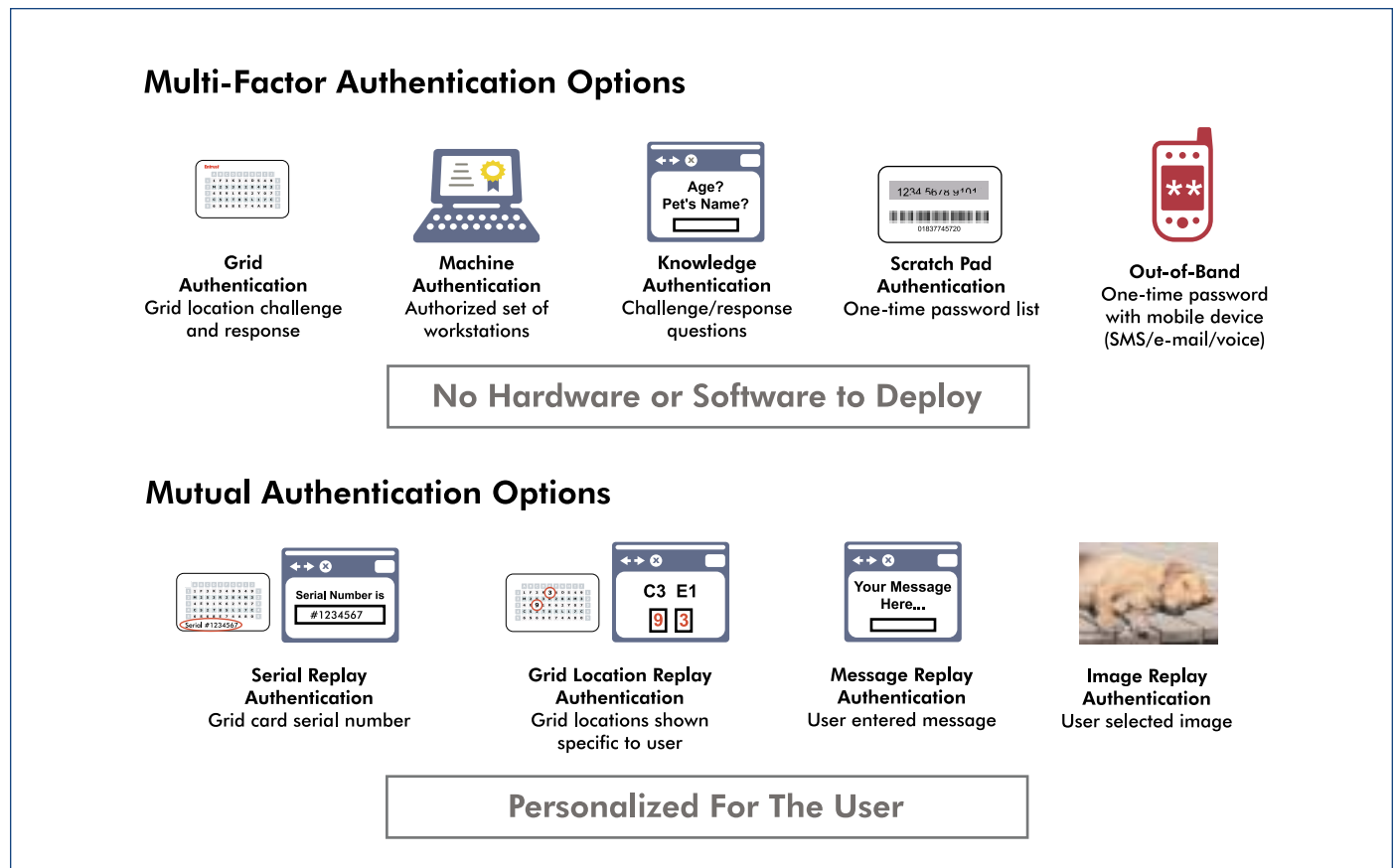


Figure 2: Entrust IdentityGuard delivers a range of highly deployable options for enterprises

The range of authentication methods provided by Entrust IdentityGuard is supported by a single administrative layer that allows organizations to manage all users through one point of policy enforcement while being able to tailor the specific authentication policy on a per-user or group basis. The security of the Entrust IdentityGuard platform is built on Entrust's FIPS 140-2 validated cryptographic engines.

**Easy-to-Use.**

Entrust IdentityGuard enables organizations to choose from a range of flexible options, all of which are familiar to end users. Independent usability tests have shown 100% success rates for Entrust IdentityGuard in the enterprise, a good representation of how easy it is for users to authenticate to sensitive applications.<sup>2</sup> The Entrust IdentityGuard authentication platform enables organizations to manage everyday authentication in the enterprise with one type of highly usable authentication, such as grid, and leverage another option, such as knowledge authentication, for applications like self-service user recovery. For organizations leveraging strong authentication for Microsoft Windows desktops, users are able work both on and offline, making it a true enterprise application for users on the go.

**Easier to Deploy.**

Entrust makes it easier for organizations to deploy strong authentication to end users, regardless of the type chosen. For grid authentication, delivering cards to end users is a seamless process, leveraging standards-based output formats for either in-house printing or production through Entrust's turnkey service. For all other types of authentication, there is nothing physical to distribute,

making deployment rapid and efficient. As Entrust IdentityGuard delivers a range of authentication methods for a single low price, the ongoing management of users through a single platform that does not charge on a per-method basis can make ongoing administration simpler and more straightforward.

**Non-invasive.**

The Entrust IdentityGuard authentication platform has been designed to work within your organization's environment with little impact to the existing infrastructure. It does not require additional client software for VPN remote access, interoperating with various leading IP-SEC and SSL VPN applications from Nortel, Cisco, Checkpoint, Juniper Networks, F5, and more. For Microsoft Windows authentication, Entrust IdentityGuard requires a small footprint client that provides the Entrust IdentityGuard grid challenge as a second step to Microsoft Windows authentication. As an authentication platform, Entrust IdentityGuard is designed to leverage your current user repository, whether it is LDAP, Active Directory, or a database, and it has been architected to address the high scalability needs of large organizations.

**Easily extends to address enterprise security.**

What makes the Entrust IdentityGuard platform unique is its ability to provide strong authentication to both enterprise and consumer environments. Not only can it be used to provide security for enterprise applications, but it can also be extended to provide highly usable, cost-effective strong authentication to multi-million user deployments that are common on the Internet today.

<sup>2</sup> Entrust IdentityGuard Usability Study, May 2005

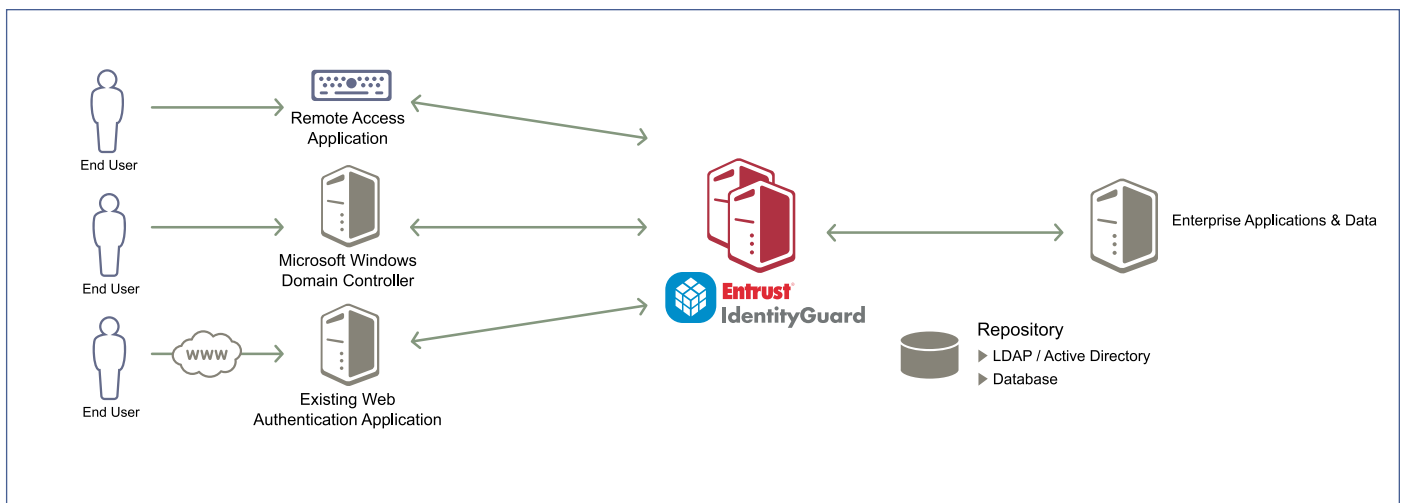


Figure 3: Entrust IdentityGuard Enterprise Architecture.

# Entrust IdentityGuard

---

## Product Architecture

The Entrust IdentityGuard solution delivers its range of authentication options to multiple enterprise applications by virtue of its design as a dedicated authentication platform. It leverages standards, including SOAP and Radius, to rapidly integrate with J2EE, .NET, or legacy applications. In addition, Entrust IdentityGuard is designed to work with existing user records in current repositories, including leading LDAP directories, such as Microsoft Active Directory, and databases from Oracle, IBM and Microsoft. Finally, in addition to a built-in web-based management console, administrative actions can be integrated into current processes via a broad set of APIs.

Entrust IdentityGuard has been developed for large-scale consumer deployments, addressing both high scale and redundancy. The architecture has been designed and tested to support transaction rates associated with large scale user deployments. To ensure availability, multiple Entrust IdentityGuard servers can be readily deployed in a load balanced environment. Performance can scale and easily be enhanced by simply adding additional servers.

## More Information

For more information on Entrust IdentityGuard, contact the Entrust representative in your area at 888-690-2424 or visit [www.entrust.com/identityguard](http://www.entrust.com/identityguard).

---

## About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please call us at 888-690-2424, or send an e-mail to [entrust@entrust.com](mailto:entrust@entrust.com). Visit us on the Web at [www.entrust.com](http://www.entrust.com).

**Entrust**<sup>®</sup> 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 2006 Entrust. All rights reserved