Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust IdentityGuard

Protecting your Enterprise

When a user logs on to the corporate network through VPN remote access or onto a Microsoft® Windows® desktop, they not only have access to the resources and information stored on the computer, but they also open a door to the corporate network and its data and applications. The security of the network and that of the desktop is only as strong as the method used to identify the users logging on. These devices either have no connection to the network or provide access online through a direct connection or over the Internet. Organizations need to consider increasing the protection of their corporate resources by improving the mechanisms for user authentication.

Usernames and passwords are considered to be one of the weakest forms of authentication used today and have proven to be subject to numerous forms of successful password attacks. One of the most effective ways to add increased security to user authentication is by using a second factor—something the user has, in addition to something they know. By adding this second factor, the odds of a successful attack on the user's user name and password can be significantly reduced.

Two-factor authentication strengthens the security of your authentication, ensuring that only you have access to sensitive information. In the past, two-factor authentication was costly and had a significant impact on the end-user experience. As a result, IT departments were often constrained in deploying it to only a limited number of users or ended up being locked into a multi-year contract for the entire employee base.

Entrust IdentityGuard for your Enterprise

Entrust IdentityGuard provides two-factor authentication that can significantly help increase the security of user authentication at a lower cost and with little impact on the user when compared to traditional methods. By providing users with something they must physically possess in order to authenticate, it makes it more difficult to maliciously obtain a user's identity. Even if an attacker obtains a user's password, they will not be able to use it without the accompanying second factor.

Product Benefits:

- **Costs less** than traditional two-factor authentication solutions
- **Easy to use** and requires only one Entrust IdentityGuard grid to authenticate to all Enterprise applications
- **Easy to deploy** and manage through standards-based design and Entrust card production services
- **Designed to fit** easily into your existing environment and supports various leading enterprise applications, including remote access VPNs

Entrust IdentityGuard

The Entrust IdentityGuard solution is inexpensive, easy to use and can be easily deployed to an entire organization at a lower cost. With a single product, your users would continue to employ their user name and password and be provided with a second physical form of authentication to log on to the network, Microsoft Windows desktop, and the Web. Entrust IdentityGuard authentication leverages a random unique grid per user that is based on an assortment of characters and numbers that could be printed on the back of an employee badge or on a plastic wallet-sized card. When logging on to the network via VPN or when logging on to your desktop through Microsoft Windows, your users would first enter their user name and password. Users would then receive an Entrust IdentityGuard coordinate challenge to demonstrate that they are in possession of their unique grid.

As illustrated for an IP-SEC integration in Figure 1, when logging on to the network via VPN, the user is first prompted for a user name and password. The user will then be asked to respond to a challenge posed by Entrust IdentityGuard, as shown in Figure 2. The challenge consists of coordinate prompts that the end user looks up on their individual grid as shown in Figure 3. In this example, Figure 4 demonstrates that the response to the challenge "A2", "C4" and "F3" is "M", "2" and "6". These numbers are entered by the end user demonstrating that they are in possession of their unique Entrust IdentityGuard grid. Use of an SSL VPN would be similar in nature but user information would all be entered through a web browser interface.

A similar approach is taken when users log on to a Microsoft Windows desktop or the Web. What is unique about Entrust IdentityGuard is that employees can use the same card to log on to the network, Microsoft Windows or the Web, thereby helping to reduce IT costs since your organization will only need to issue one card for all applications requiring authentication.

Entrust IdentityGuard Advantages

Secure. Adding grid-based authentication to passwords can help to significantly improve the security of user identities. A simple 5 x 10 alphanumeric format provides a virtually unlimited set of unique grids and over 19,500 three-location challenges with more than tens of thousands of potential responses to each. The result is security that is over 10 times more resistant to attacks than passwords alone. Perhaps equally important, organizations may avoid attacks simply by virtue of deploying a solution that makes them less vulnerable and, thus, a less attractive target.

Lower Cost. Compared to traditional two-factor authentication solutions, Entrust IdentityGuard helps provide a lower cost option. Your organization can choose the distribution method that is most cost effective and convenient, such as printing the unique grids on the back of employee badges or on a simple wallet-sized card.

Figure 1 Figure 2 Figure 3 Figure 4

Easy to Use. The grid-like, challenge-based authentication mechanism is simple for users to understand as it is similar to a map navigation lookup where users respond with the grid cell contents that correspond to the challenge coordinates.

Entrust IdentityGuard enables a flexible form factor that can be as simple as a wallet-sized plastic card which is easy to carry and use. It can even be adapted with features such as raised Braille print to accommodate a diverse user population. Should a user lose or misplace their unique grid, Entrust IdentityGuard also provides the ability to use a temporary passphrase for strong authentication in case of emergency. The temporary passphrase is available to users whether they are connected to the network or not.

Easier to Deploy. Entrust makes it easy for organizations to produce and deploy cards to users through standards-based output formats, either through in-house printing facilities or Entrust card production services. Entrust card production services works with you to produce Entrust IdentityGuard cards for your users. Entrust can make it easy for you to produce your cards at a low cost without incurring the cost of implementing a secure and audited card manufacturing process in-house. You are able to renew your card orders from your account on the Entrust Extranet, making deployment faster and easier.

Extensible. The Entrust IdentityGuard solution can be used as a second factor of authentication for all Enterprise applications such as IP-SEC and SSL VPN remote access, corporate intranet, and Microsoft Windows. Unlike other two-factor authentication methods, the Entrust IdentityGuard solution does not require that specialized hardware be distributed to end-users. It can also be leveraged across multiple channels and integrated with systems such as automated voice response applications that allow users to be authenticated when calling in to help desks and other telephone services.

Non-invasive. The Entrust IdentityGuard system has been designed to work within your organization's environment with little impact to the existing infrastructure. Entrust IdentityGuard leverages the Radius protocol and SOAP to allow for rapid configuration and deployment. Entrust IdentityGuard does not require additional client software for VPN remote access as it is designed to operate with various leading VPN applications offered from Nortel, Cisco and Juniper Networks. For Microsoft Windows authentication, Entrust IdentityGuard requires a small footprint client that provides the Entrust IdentityGuard challenge as a second step to Microsoft Windows authentication. It is designed to use your current repository whether it is LDAP, Active Directory, or a database, and it has been architected to address the high scalability needs of large organizations.

Product Architecture

The Entrust IdentityGuard solution is centered on a server-based software product that can be installed in an organization's current Web infrastructure. It is a J2EE application and is deployed on the Linux operating system. The Entrust IdentityGuard server component is designed so that it may be tailored to an organization's environment, providing an interface to receive calls from applications in order to add the second factor of authentication. Likewise, an interface is provided for the user repository for the purpose of storing and retrieving card information. The product is designed to meet the scalability requirements of large organizations, with support for redundancy and load balancing.

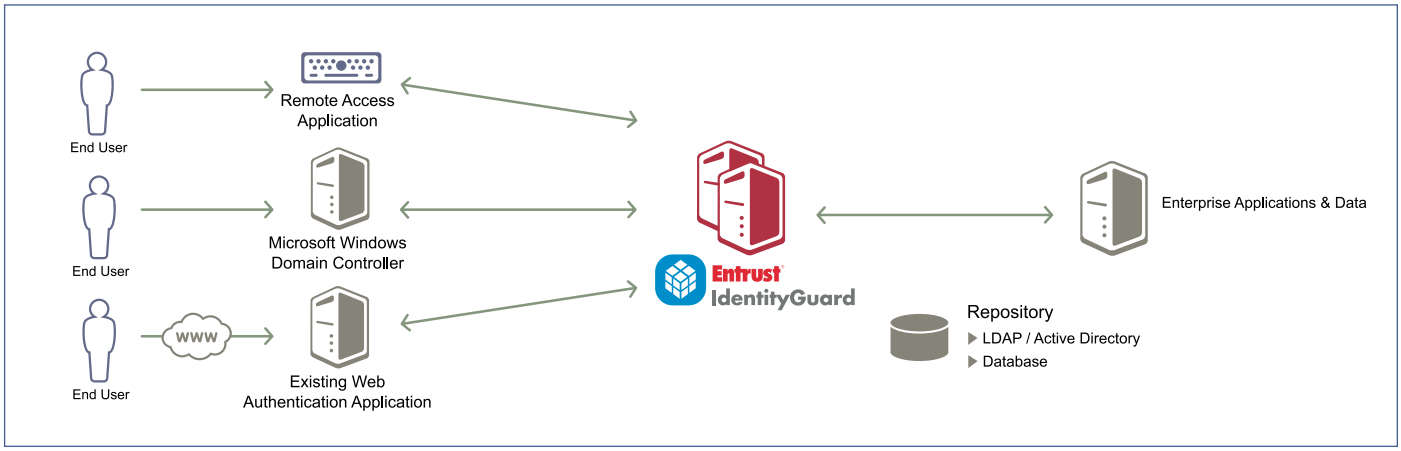

Figure 4: Entrust IdentityGuard Enterprise Architecture.

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. Visit us on the Web at www.entrust.com.

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 2005 Entrust. All rights reserved