

# Entrust IdentityGuard

To reduce the risk of illegitimate access to networks and intellectual property, corporations need to deploy stronger forms of network and application authentication. User names and passwords are no longer sufficient to protect enterprise data.

Entrust IdentityGuard provides two-factor authentication that can significantly help increase the security of user authentication at a low cost and with little impact to users when compared to traditional authentication 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.

The solution can be easily deployed to an entire organization at a lower cost than battery-powered tokens. With a single product, users would continue to employ user-names and passwords and be provided with a second physical form of authentication to remotely access the enterprise network, Microsoft Windows desktop and Web-based applications. Entrust IdentityGuard is ideal for providing physical/logical security convergence via a single physical card.

Entrust IdentityGuard authentication leverages a random unique grid per user that is based on an assortment of alphanumeric values that could be printed on the back of an employee badge or on a plastic wallet-sized card. When logging on, users would first enter their user name and password as usual, and then receive a coordinate challenge to demonstrate that they are in possession of their unique grid, thus verifying their identity.

What is unique about Entrust IdentityGuard is that employees can use

the same physical card to log on to the network, VPN or Web applications that they use for facilities access, thereby reducing costs since an organization only needs 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.

**Lower Cost.** Compared to traditional two-factor authentication solutions, Entrust IdentityGuard helps provide a lower cost option both in terms of product license costs and on-going administrative costs.

**Easy to Use and Deploy.** The grid-factor, 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. Flexible deployment allows organizations to choose the most ideal distribution method, such as printing the grids on wallet-sized cards or on the back of employee badges, creating a single method of both physical building access as well as logical access.

**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 login. It does not require that specialized hardware be distributed to end-users. It can also be used across multiple channels including automated voice response (IVR) applications that allow users to be authenticated when calling 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. It leverages the Radius protocol and SOAP to allow for rapid configuration and deployment. Entrust IdentityGuard operates with leading VPN solutions including Nortel, Cisco and Juniper Networks. It is designed to integrate into existing LDAP, Active Directory, or database repositories, and it has been architected to address the high scalability needs of large organizations.

By making an investment in this single mechanism, an organization could provide greater security across the numerous ways it communicates with its users, simplifying user experience and helping to reduce expenses. **SB**