

## Securing the Connection with Remote Users

*Leveraging Strong Authentication and VPNs to Secure Access to the Enterprise*

Organizations today are feeling increased pressure to lower the costs of doing business. As a part of addressing that pressure, many organizations have implemented Virtual Private Networks (VPNs) to provide remote users with the access to the corporate resources that they need at dramatic cost-savings over previous methods.

This whitepaper discusses the various authentication mechanisms available for VPNs and outlines how strong authentication based on digital IDs can help organizations realize cost savings and increase service levels for users while maintaining high levels of security.

June 2004

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. 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 and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. You shall be solely responsible for acting or abstaining from acting based upon the information in this document. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS DOCUMENT. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

## Table of Contents

|            |  |           |
|------------|--|-----------|
| <b>1</b>   | <b>Introduction</b> .....                                | <b>1</b>  |
| <b>2</b>   | <b>Virtual Private Networks for Remote Access</b> .....  | <b>1</b>  |
| <b>2.1</b> | <b>Private Networks</b> .....                            | <b>2</b>  |
| <b>2.2</b> | <b>The Internet – a Public Network</b> .....             | <b>2</b>  |
| <b>2.3</b> | <b>Virtual Private Networks</b> .....                    | <b>2</b>  |
| <b>2.4</b> | <b>VPN Challenges</b> .....                              | <b>2</b>  |
| 2.4.1      | Basic and Strong Authentication.....                     | 3         |
| 2.4.2      | Weaknesses in Password Authentication .....              | 3         |
| 2.4.3      | Alternatives – Time-synchronous Tokens .....             | 4         |
| <b>2.5</b> | <b>Certificate-based Authentication</b> .....            | <b>5</b>  |
| <b>3</b>   | <b>Entrust Secure Identity Management Solution</b> ..... | <b>6</b>  |
| <b>3.1</b> | <b>Strong Authentication for VPN Solutions</b> .....     | <b>7</b>  |
| <b>3.2</b> | <b>The Business Benefits</b> .....                       | <b>8</b>  |
| <b>4</b>   | <b>Entrust Solution Components</b> .....                 | <b>9</b>  |
| <b>4.1</b> | <b>Strong Authentication for VPN</b> .....               | <b>9</b>  |
| <b>4.2</b> | <b>Secure User Provisioning</b> .....                    | <b>9</b>  |
| <b>5</b>   | <b>The Need to Act Now</b> .....                         | <b>10</b> |
| <b>6</b>   | <b>About Entrust</b> .....                               | <b>10</b> |

# 1 Introduction

In today's competitive environment real-time communication between subsidiaries, offices and employees around the world is imperative. Additionally, an ever-growing remote workforce requires access to the corporate applications and information they need to perform their jobs. As a result, organizations have implemented Virtual Private Networks (VPNs), which leverage secure connections over the Internet. VPNs provide remote workers and offices with anytime, anywhere access to the corporate network at dramatic cost-savings versus dial-up access or leased lines from telecommunications carriers.

VPNs allow an organization to easily build, manage and operate low-cost private networks using the Internet to connect mobile and remote workers, remote offices and branch offices more efficiently. Leveraging the Internet allows the organization to extend remote access to more employees, helping to improve overall employee productivity and ultimately helping to drive greater efficiencies and returns. VPNs are a particularly attractive option for organizations that have large numbers of remote users and /or multiple locations to connect to the main corporate network.

Since VPNs provide a door from the Internet into the corporate network and all its resources, security is of the utmost importance. The security of the network is only as strong as the method used to identify the users or devices at each end of the communication. Many options are available to verify the identity of the user accessing the VPN, each of which provide different levels of security and manageability. These range from username/passwords to time-synchronous passwords and tokens and certificate/private key based digital IDs.

By delivering and managing digital IDs for strong identification of users and devices communicating and exchanging information over a VPN, Entrust<sup>®</sup> products provide security for organizations deploying VPNs. Entrust products allows them to provide access to a full range of sensitive information, enabling organizations to unlock the promise of VPNs, while reducing user deployment and maintenance costs.

This paper outlines the value of VPNs as a remote access solution. It highlights the benefits and drawbacks of enabling remote access over the Internet as opposed to using a private network. The discussion will then focus on the challenges found in simply using commercial off-the-shelf VPN solutions from two perspectives:

1. the security of the off-the-shelf solution with a focus on authentication security, and
2. the deployment of the VPN solution with a focus on user management.

After discussing the challenges, the available solutions will be outlined with a focus on strong authentication and the role it plays in securing access to an organization's sensitive applications and data. The paper will conclude with an overview of how Entrust products deliver strong authentication for VPN deployments, and the role these products play in the Entrust<sup>®</sup> Secure Identity Management Solution.

## 2 Virtual Private Networks for Remote Access

The benefits of allowing mobile and remote employees to access their corporate infrastructure while working from home or while on the road are widely recognized for the added productivity it delivers. Remote access delivers the applications and information that employees need to continue the flow of business information wherever they are, whenever they need it.

## 2.1 Private Networks

Traditional methods of providing mobile and remote employees with access to corporate systems and information made use of leased lines and dial-up infrastructures. Costs incurred from the deployment of such systems comprise the cost of permanent leased lines, local or long-distance telephone connections, and the internal systems required to handle access to the corporate network. These costs are substantial and the performance of these connections is lackluster. However, since these connections establish a private connection between the remote or mobile user and the corporate infrastructure, security threats are minimal.

## 2.2 The Internet – a Public Network

The emergence of the Internet provided an excellent alternative to point-to-point private networks outlined above for electronic communications and information exchange. The network is supported by a robust, high-performance and highly available infrastructure that is available to anyone, anywhere, at anytime. The beauty of the Internet is that it is a public network; however, the Internet's design has security flaws and is fraught with peril as demonstrated by regular reports about security vulnerabilities and threats. CERT, a reputable centre of Internet security expertise hosted by Carnegie Mellon University, reports that:

- Internet security incidents rose from 6 in 1988 to 137,529 in 2003, and
- Reported vulnerabilities rose from 171 in 1995 to 3,784 in 2003. (For more information on the top security vulnerabilities see "The Twenty Most Critical Internet Security Vulnerabilities", SANS Institute, 2000-2003, <http://www.sans.org/top20/#threats>)

## 2.3 Virtual Private Networks

Virtual Private Networks address some of the security problems associated with communicating and exchanging information over the public Internet by securing the communications between the two end-points. In fact, VPNs establish a secure tunnel between these two points so that information exchanged is protected against being intercepted, modified, stolen or otherwise compromised. It does this over the Internet by establishing a virtual secure channel; a virtual private network protecting internal networks and the applications and information they contain.

### Increased Productivity and Cost Benefits

The significant benefit of VPNs is that they allow organizations to take advantage of the Internet to help reduce the communication costs of remote users and branch offices. Internet access is relatively inexpensive compared to that of dedicated leased lines or the cost of establishing local and long-distance telephone connections. In addition, a single corporate infrastructure is required to accommodate VPN access, regardless of the method used by the mobile or remote user to connect to the Internet such as dial-up, cable modem, ISDN, ADSL, etc. These lower costs combined with the productivity benefits of having resources available from anywhere, anytime to all mobile or remote users translate to definite savings and a high return on investment.

## 2.4 VPN Challenges

Although VPN technology promises to resolve a number of the issues related to Internet security, and reduce the cost of deploying a remote access system to mobile and remote users, its inherent capabilities out-of-the-box introduce some challenges:

- Default authentication mechanisms offer limited security, and
- User enrollment and management functionality can become cumbersome and costly as the number of deployed users and remote offices increases.

## 2.4.1 Basic and Strong Authentication

One of the keys to Internet security is authentication: making sure that users accessing your corporate network are indeed who they say they are. Basic VPN authentication often only uses a username/password. Usernames and passwords are considered to be single factor for authentication and one of the weakest forms of authentication used today. The more difficult it is to impersonate a user by forging or faking the means of authentication, the stronger the authentication mechanism is.

### Authentication Categories

**What you know** - Knowledge-based authentication mechanisms rely on users' memories, requiring them to memorize secret information that can be used to prove their identities to an authentication system. In its most popular form this knowledge takes the shape of a username/password. Close relatives include the Personal Identification Number (PIN) and passphrase. Such methods of authentication are also classified as **single-factor authentication** and offer very basic security. Adding security to authentication requires the addition of other "factors" to the authentication process.

**What you have** - Possession-based authentication mechanisms require users to physically control an object or device. This device may connect directly to an authentication system, or it may require users to input information. Examples range from magnetic and radio frequency (RF) cards to smart cards. Also included in this category are one-time password tokens, USB tokens, and digital certificate/private key pairs. These methods of authentication are also referred to as **2-factor authentication**.

**What you are** - Biometric-based authentication mechanisms work by taking measurements of unique physical or psychological human traits. Popular mechanisms include fingerprints, hand geometry, iris patterns, voiceprints, and facial geometry. Mechanisms that require physical characteristics are referred to as **3-factor authentication**.

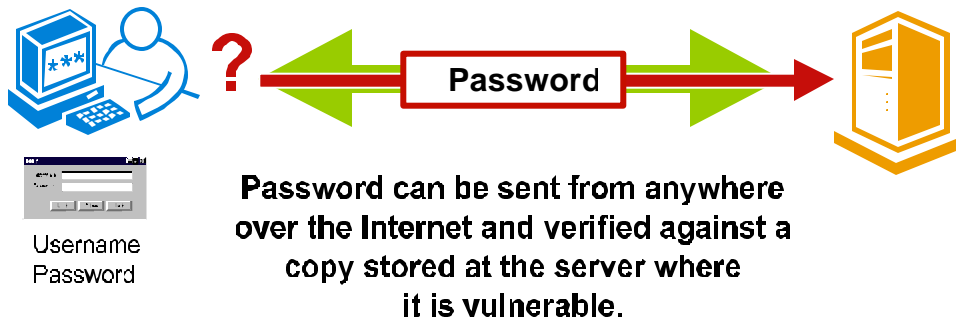
## 2.4.2 Weaknesses in Password Authentication

Password-based authentication mechanisms contain a number of inherent security weaknesses as well as significant challenges in deployment (user registration and provisioning, and single-application authentication) and ongoing management (such as password resets and password change policies). Compromised passwords are among the most common security vulnerabilities to systems that base user authentication on this single factor. Users are often careless with their passwords and password policies are difficult to enforce. Attackers have plenty of tools for defeating password protection and these can be both technical and social. Once an attacker has a user's password, he or she has all of the rightful user's privileges. Should the user have access to corporate resources via a VPN, the compromised password will give an attacker access to those same resources.

The selection of a weak password is the most common security vulnerability and will likely be the primary source of security breaches. Adding strength to passwords will somewhat mitigate the risk, but tools are readily accessible to compromise these. The following are the most common threats and attacks on password security:

- **Lack of user care** leads users who either have multiple passwords to write the passwords down on paper or other readily accessible media.

- **Poor password selection:** The selection of a weak password, such as a favorite pet's name, leaves passwords vulnerable to guesses and dictionary attacks. Password guessing involves entering common passwords either manually or through programmed scripts.
- Passwords are **stored in cleartext** on local and network devices, and thus are often easy for administrators and rogue users to find.
- Temptation exists for users to use the **same password/shared secret across multiple devices and applications** to simplify management -- this increases the likelihood of compromise and the scope of risk.
- **Social engineering** attacks demonstrate that it is still surprisingly easy to obtain users' passwords by simply asking them. Social engineers masquerade as administrators or other authoritative roles to convince users to tell them passwords.
- **Brute-force logon attacks** follow the same basic logic as password guessing but are much faster and more powerful. Very large dictionaries and user lists are available as well as the tools to automate the process. Brute-force attacks are more efficient than password guessing but both techniques are essentially the same.
- **Password sniffing** uses tools that grab passwords "off-the-wire" as they are passed from the desktop to the authenticating server. VPNs and Web authentication are particularly vulnerable to this type of attack because passwords are often passed in cleartext over the public Internet.
- **Password cracking** is a much more effective method for discovering passwords and circumvents the lockout defense by enabling the offline brute-force cracking of passwords. This commonly requires an attacker to penetrate the access device and then gaining elevated privileges. It is to be noted that a number of readily available tools Lp0phtcrack, LC3 and John The Ripper have made the process of cracking passwords quite trivial unless users are very careful to use very difficult passwords to crack. These would likely include special characters such as "@&#.



### 2.4.3 Alternatives – Time-synchronous Tokens

Alternatives such as time-synchronous hardware tokens are available to address the weaknesses of simple password authentication. These proprietary hardware tokens are used to authenticate to the VPN by leveraging a synchronized time code. Such schemes provide greater security than passwords alone, as they require users to be in physical possession of the token. However, this greater security comes at the price of ease of use, requiring the physical distribution, use and management of hardware devices. In addition to significant usability issues, hardware tokens are also limited in terms of flexibility:

- Most organizations will assign specific access rights to users to reflect the groups to which they belong and the importance of the resources to which they have access. As such, some users will require higher authentication security than others given their job responsibilities. With token-based authentication solutions, each user would have the same level of authentication strength regardless of requirements. Digital IDs provide much more flexibility while still providing greater security than password-based authentication. Users performing more sensitive operations can use their digital IDs that are stored on a smart card to enhance the security, while others may simply use their digital IDs stored on their local hard drives.
- Another limitation of tokens is their inability to be used for anything other than authentication. As discussed previously, the accountability of users' actions pertaining to their access to important information and applications is critical. Increasingly, digital signatures and encryption will be used to enhance accountability for each part of the workflow required for issuing identities and application access rights. This includes functionality, such as secure e-mail, to protect automated workflow among administrators, or digitally signed transactions and audit logs for integrity. Digital IDs can be used by administrators for these functions, while tokens remain restricted to authentication. For organizations deploying identity management, digital IDs provide the immediate benefit of strong authentication, with the added benefit of being able to implement additional security measures over time without the need to deploy additional systems.

## 2.5 Certificate-based Authentication

Because a VPN can open access to sensitive and valuable corporate data, applications and other resources, it is important to be able to securely identify each end of the communications tunnel. Recognizing that passwords are not sufficient to protect the sensitive and valuable corporate resources made accessible by a VPN, a secure solution must provide:

- Strong and secure identification of users/devices;
- Verification of communications; and
- Comprehensive and secure management of the user/device identities, including enrollment and ongoing management.

Authentication based on a digital ID composed of certificates and private keys is widely recognized as one of the most secure means of authentication available today. As an organization's VPN requirements grow to involve more users and more devices, Entrust products help manage the security of these users and devices in a way that can allow for ongoing cost savings and reduced risk of unauthorized access or misuse.

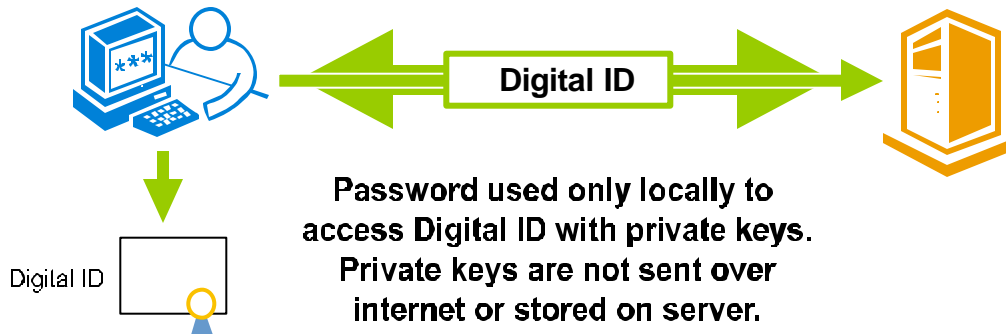
Leading VPN product vendors support certificate-based authentication and the infrastructures that issue and manage certificates and their associated keys. This integration is the key to delivering certificate-based strong authentication to remote access.

A digital ID addresses the weaknesses of password authentication as follows:

- A digital ID includes cryptographic keys and certificates that must be physically in the possession of the user in order for him or her to authenticate – it is a second factor for authentication. As such, even if someone was to obtain a user's password through one of the vulnerabilities cited above, the attacker could not exploit it in the same way as with just a user's name and password. The attacker would require physical access to the

digital ID. A rogue employee or attacker cannot simply take the password and attempt to access the VPN and corporate network from another workstation.

- Although there is a password associated with a digital ID, it is only used locally on the user's workstation to authenticate—it never travels over the network. In addition, the fact that a digital ID is not centrally stored eliminates the vulnerability of a rogue user accessing the central store to obtain information that could be used to subsequently impersonate another user or even an administrator.



In summary, digital IDs provide strong security to protect resources made available to mobile and remote users through a VPN, while addressing the weaknesses of password authentication and enabling a flexible approach to the security requirements of identity management.

### 3 Entrust Secure Identity Management Solution

Entrust provides a comprehensive, highly-scalable secure identity management solution that can help customers easily deploy and manage identities for **strong authentication** to VPN infrastructures for a broad range of client-server, Web, and Web services environments including for strong authentication to VPN infrastructures. Focused on addressing the challenges of commercial and government organizations, the solution enables organizations to lower the costs associated with managing user, application, and device identities across heterogeneous, complex environments. Through best-of-breed capabilities for securely deploying and managing identities, the solution helps to improve return on investment for organizations, providing rapid deployment, easy and secure administration, and scalability to address the large user populations.

With the **Entrust Secure Identity Management Solution**, IT administrators can provision a unique ID to every VPN user and to every application within the enterprise. One single identity management systems allows individual permissions, privileges and profile data to be managed across a complex matrix of applications and systems. Furthermore, access to the identity management system is strongly secured, user data is protected, and information workflow can be audited for overall accountability.

No less important than a clear understanding of the security requirements of a VPN deployment and the inherent weaknesses of the basic authentication offered out-of-the-box by VPN vendors is the cost of deploying and ongoing maintenance of usernames/passwords as a means of authentication. By design, usernames and passwords offer very little scalability and place

infrastructure and application administrators in the face of serious management challenges. A strong identity management solution can allow organizations to enable VPN users quickly by addressing issues such as:

#### **User Enrollment**

In order to make VPN user enrollment simple and cost-effective, administrators need tools to manage user registration and the distribution of digital identities for authentication. VPN products do not offer tools to easily distribute usernames and passwords to users. Administrators must assign usernames and passwords manually to each VPN user and device.

#### **Self-service Enrollment**

If administrators want to accelerate enrollment, enable enrollment from anywhere, anytime, and reduce costs even more by reducing administrative duties, they require Web-based self-service tools. VPN products do not offer such products for user self-registration.

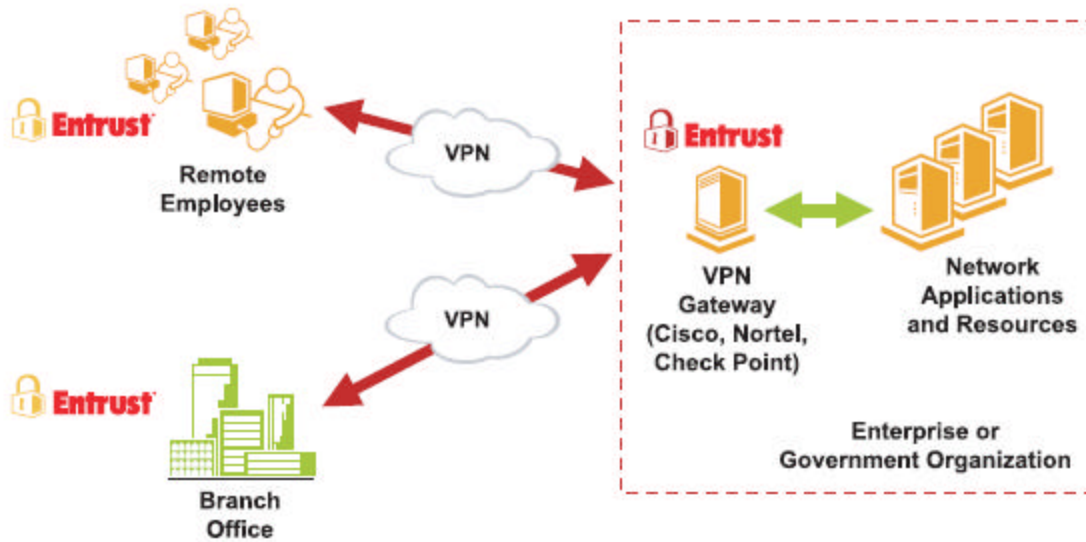
#### **Forgotten Passwords**

The help-desk costs associated with the reset of forgotten passwords are widely documented and a potential burden on any organization that chooses to use password authentication. VPN products do not offer self-service tools for password recovery.

### **3.1 Strong Authentication for VPN Solutions**

As an inherent part of the Entrust Secure Identity Management Solution, Entrust delivers the ability to leverage digital IDs for VPN authentication, adding critical strong authentication to off-the-shelf VPN products to provide:

- **Increased security:** through strong identification of VPN users and devices, including verification that the user/device is currently authorized to connect to the VPN. Strong certificate-based authentication is achieved through Entrust® digital identities (digital IDs).
- **Flexibility in private key protection:** The Entrust digital IDs composed of certificates and keys can be stored on desktops, smart cards or tokens, or on a central directory for roaming access.
- **Reduced user administration:** users are able to register and perform basic self-administration tasks independently and securely, including password resets and the recovery of digital IDs.
- **Increased scalability:** the use of Entrust digital IDs for strong authentication of users can reduce VPN security administration when compared to using username/password or pre-shared key implementations.
- **Ease of use:** security functions are transparent and easy to use for the end user and security management tasks are automated for administrators.
- **A single security infrastructure for various VPN products:** the award-winning Entrust public-key infrastructure can provide enhanced security and secure identity management for today's market leading VPN products.
- **A single security infrastructure for strong authentication to multiple applications:** Entrust digital IDs can be used with authentication applications that support certificate and key-based authentication, including Windows Smart Card Logon, 802.1x certificate-based authentication, and two-way SSL authentication to Web servers.
- **A single security infrastructure for digital signatures and data encryption across applications:** the same Entrust digital ID can also be used with applications that support x.509 certificates for encryption and digital signatures. These security features are supported by leading e-mail and data protection applications.



### 3.2 The Business Benefits

Working closely with customers to understand and recommend how to address identity and access management challenges within the enterprise, Entrust delivers a solution that can help to:

#### Increase organizational efficiencies and reduce IT costs

- Moving away from traditional 'stove-pipe' systems management to centralized management of identities across all applications can help reduce IT administration cycles. Dedicated VPN user management systems and processes are no longer necessary.
- Entrust's Secure Identity Management Solution provides enterprise single sign-on and automated identity lifecycle management to ease Help desk costs and increase user satisfaction.
- Entrust's unique architecture and tightly integrated identity management components can help enable rapid deployment of applications and thus improve project delivery.

#### Improve compliance with legislative and corporate governance requirements

- centralized provisioning and single point of access control for applications can help to enforce corporate policies
- strong authentication and access controls management can help enable organizations to deploy sensitive applications with the confidence that authorized users and applications will have the ability to retrieve the information
- the ability to add digital signatures and encryption through the same authentication point can help allow organizations to grow to new applications without deploying a new infrastructure

#### Increase service levels and user satisfaction

- single sign-on can help enable users to easily and more rapidly access their applications and data, regardless of where they are - on-site or accessing the corporate network remotely

- user self-service for identities (for tasks such as password reset or user profile updates) empowers users to act on needs themselves without relying on the Help desk

#### **Enable secure collaboration among employees**

- leading authentication capabilities (including two-factor authentication using Entrust USB Tokens) help to provide positive identification of user and application identities
- strong authorization functionality manages resource access control across both internal networks and over the WLAN/VPN
- digital signatures and encryption can help improve accountability and privacy for information and transactions

## **4 Entrust Solution Components**

### **4.1 Strong Authentication for VPN**

Working with leading VPN vendor products, Entrust<sup>®</sup> VPN Security utilizes the strong security capabilities that are provided by two flagship Entrust<sup>®</sup> product portfolios:

The **Entrust Intelligence™** portfolio of desktop security products delivers a managed Entrust digital ID, allowing all key and certificate updates, maintenance of key histories, key backups, revocation checks and name changes to occur automatically, without the user's involvement. The managed digital ID enables digital signature, encryption and authentication capabilities across a wide variety of desktop applications that allow organizations to protect the privacy and integrity of corporate data. The Entrust Intelligence portfolio also secures the Entrust digital ID so that only the authorized trusted user can access it to conduct secure operations.

**Entrust<sup>®</sup> USB Tokens** work seamlessly with Entrust digital IDs to deliver strong two-factor authentication of users to the Web/Web Services environment. Entrust digital IDs can also be stored and managed on smart cards from the leading vendors.

**Entrust Authority™** provides the backbone of the PKI. They issue digital identities to users and devices and deliver the security management capabilities that can help make VPN security deployments more scalable and easier to manage.

### **4.2 Secure User Provisioning**

**Sun<sup>®</sup> Identity Manager** provides centralized identity administration across the Web/Web services architecture. It can securely and efficiently deploy and manage identities, and delivers automated identity provisioning, centralized password management, single-step identity profile management, robust auditing of the identity infrastructure and flexible workflow.

**Entrust GetAccess™** delivers policy-based access control and Web Single Sign on (SSO) for Web portals. It is used across both administrator and user environments to secure and streamline access to identity information. Proven in deployments with millions of users, Entrust GetAccess also provides robust access controls to both internal and external portal applications.

**Entrust TruePass™** is a "zero-footprint" that leverages Entrust digital IDs to provide easy-to-use, integrated strong authentication of users to sensitive applications, including the identity administration portal.

## 5 The Need to Act Now

Organizations today are feeling increased pressure to lower the costs of doing business. As they leverage the Internet and enterprise networks to streamline business processes, they are experiencing an increasing need to find new ways to service employees, partners, suppliers, and customers who are demanding real-time, personalized access to information. Whether this means allowing partners to deeply integrate with their supply chain management system, or allowing customers to access confidential account information online, organizations must effectively extend the boundaries of their enterprise to remain competitive, without compromising the security of their networks and resources. At the same time, organizations need to manage the identities of the increasing number of end-users that are accessing applications.

Building on over 10 years of experience with Global 1000 companies, Entrust has assembled a comprehensive solution that is unmatched in the industry. The Entrust Secure Identity Management Solution is the right choice when it comes to giving employees, customers and partners secure access to information and resources needed to conduct business.

Entrust products are unique in their ability to manage identities and access across the enterprise, delivering strong authentication capabilities for remote access and other applications. These capabilities can easily be enhanced by the modular capabilities of the Entrust Secure Identity Management Solution for authorization and SSO, and provisioning capabilities for users, applications, and devices. The solution includes features that enhance security and overall accountability for organizations, including a robust auditing system that enables organizations to review transactions.

The longer an organization waits to adopt a secure solution for remote access, the greater the risk of compromising secure information and putting the company in a state of non-compliance with legislation that has severe penalties for both individuals and corporations. The Entrust Secure Identity Management Solution delivers a comprehensive set of best-of-breed capabilities for secure, effective control over users and their access to enterprise resources.

Furthermore, Entrust services and supports this tightly integrated solution through its specialized best-in-class global support organization, helping to enable organizations to rapidly deploy and utilize the solution. The enterprise that acts quickly to incorporate these capabilities in its operations can reduce its risk, and lower its costs while improving relationships with employees, partners, suppliers and customers.

For more information on the Entrust Secure Identity Management Solution, please visit:

[http://www.entrust.com/identity\\_management/](http://www.entrust.com/identity_management/)

## 6 About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world-leading provider of Identity and Access Management solutions. Entrust software enables enterprises and governments to extend their business reach to customers, partners and employees. Entrust's solutions for secure identity management, secure messaging and secure data increases productivity and improves extended relationships by helping to transform the way transactions are done online. Over 1,250 organizations in more than 50 countries use Entrust's proven software and services to turn business and security challenges into secure business opportunities. For more information, please visit:

<http://www.entrust.com>.