aep NETWORKS

The **specialist** in network and application access security

WHITE PAPER

AEP Smartgate® Security

Strong Multi-Factor User Authentication for Secure Information Sharing

Introduction

The long-standing practice of building private information networks by leasing dedicated circuits has virtually disappeared due to advances in networking technology and economies of scale realized by the Internet. Today, enterprises are seeking solutions that allow secure "anytime-anywhere" access using the Internet to increase productivity and reduce costs. Virtual Private Networks (VPNs) have become the accepted method of securing data for transport over a public network, connecting with business partners and enabling remote access. But the truth is, all VPNs are not created equally.

There is plenty of confusion when one delves into the world of VPN security because of its complicated nature, plethora of offerings, and misinformation. While many solutions on the market today are adept at encrypting data between two points, they fall short when it comes to ensuring that end users can be trusted and are only able to access appropriate resources. SSL VPN products traditionally include rudimentary one-factor password protection systems that only provide minimal protection and can easily lead to a false sense of security. Without the confidence of knowing who is on the end of a connection, security cannot be assured—which is the reason for deploying a VPN in the first place.

This paper is intended to give the reader a high level appreciation for the importance of strong user authentication, an area critical to security in networked systems and VPNs, yet so frequently misunderstood. It will provide a high level overview of identity and access management mechanisms employed by AEP Networks' AEP Smartgate®, which can act as a complementary user authentication add-on along side an installed VPN or operate as a fully functional standalone application layer VPN.

AEP Networks is a pioneer in the development of secure remote access, application protection and user authentication solutions using application layer SSL VPN technology. At the core of AEP Smartgate is a highly secure multi-factor authentication system that can operate by itself or be simply linked with third-party authentication products. AEP Smartgate ensures that only positively identified, authenticated users are permitted to access information they are entitled to view and/or control.

Password Protection

Nearly everybody who has used a networked computer is familiar with simple user ID/password security, a protection scheme in which a person must enter a valid string of alphanumeric characters in order to gain access to information and resources. If the combination submitted matches the associated record stored in an authentication database, access is granted. Straightforward, simple and practically "free," password protection systems are used by most SSL VPN solutions on the market today. They are, however, minimally effective as a deterrent against unauthorized access, suffer from numerous shortcomings and are susceptible to a variety of single-factor attacks. While almost all IT managers are knowledgeable about password limitations and problems, many organizations have still not upgraded antiquated systems or taken this issue seriously for various reasons, including the perception that addressing password security is a resource intensive and costly endeavor.

In most cases, passwords can be guessed or deduced in a short period of time—sometimes seconds—using readily available public domain software cracking utilities. A paradox exists in that having users select their own passwords makes the strings easy to remember, but also simple to guess; and conversely, enforcing rigorous password composition rules makes the strings difficult to crack and hard to remember. Ironically, strict password security policies typically result in less secure and more costly systems. Requiring users to change their passwords frequently and enforcing the use of hard-to-guess strings usually means people will write down their private passwords, record them on "sticky notes," or store them in an electronic file, usually in obvious or easy to access locations. This is especially true when a user has to manage user ID/password combinations for numerous systems and accounts.

Rigorous password policies correlate to an increased number of support desk calls that are costly and should not be overlooked. On average, a password reset or assistance call costs a company approximately $25, though some reports claim the number can exceed $50 per occurrence. The Gartner Group estimates that over one quarter of all support desk calls are related to passwords. Aberdeen places annual labor costs for configuring and managing password systems at $100+ per user for small companies and up to $300-350 per user in large enterprises. These ongoing expenditures mount rapidly and are not insignificant.

A serious weakness with passwords, illustrated in Figure 1, is that they must be transmitted across a network, often the public Internet, every time access is needed. Even though the confidential password string is almost always encrypted, it still must traverse a medium where interception and decryption is possible. While most cryptographic algorithms available today are extremely difficult to crack, it should be noted that many SSL products still rely on relatively weak 128-bit encryption. A determined hacker can capture scrambled data packets and, with sufficient motivation and resources, invest the time, money and energy to decipher them. Though changing encryption keys are frequently used which makes the job more difficult, a hacker knows that once a password is obtained, it can be used over and over again for access, since the holder is assumed to be authorized.

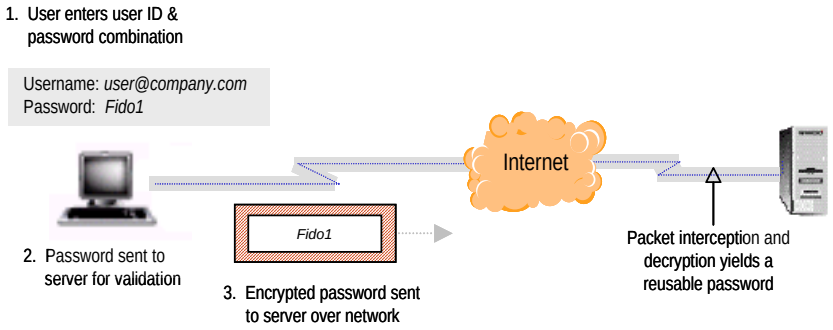

Figure 1: Passwords Must be Sent Across a Network to be Validated

There is a wealth of information available today, particularly on computer hacker discussion boards, that describes how surprisingly simple it is to obtain user passwords through technology, social engineering or just relying on predictable human behavior. Computer security professionals agree that use of passwords as the only protection mechanism in a sensitive environment is often inadequate and ill-advised. Virtually every major industry analyst firm including Aberdeen, Forrester, and Gartner all warn that static passwords are one of the most serious security threats facing organizations today. The Government Accountability Office (GAO) has even gone on record with a recommendation for Federal agencies stating:

> *Security assurances beyond passwords are needed to protect sensitive, financial and personal data transferred via the Internet during communication and transactions among government employees and business partners and the federal government.*

Two-Factor Authentication & Access Codes

Consider for a few moments the ubiquitous automated teller machine (ATM) that banks have successfully employed for years. Financial institutions realized long ago that a password-only approach was vulnerable to attack and just too weak to protect their monetary assets, so they turned to the more powerful two-factor model.

A two-factor authentication system is based on two required elements, both of which must be present at the time of validation:

❶ Something you have in your possession (i.e., a valid bank card); and,
❷ Something you know that can be memorized (i.e., a personal PIN code).

The combination of these two factors is required to gain access to an account and is orders of magnitude more secure than a password-only approach. In effect, the system is asking for two types of user identification before granting access. A bank card is of no value without the corresponding PIN (Personal Identification Number); the same logic applies to a compromised PIN, in that account access is not possible without the associated bank card.

It should be understood that a user ID/password combination does not constitute two-factor security since only one of the two required elements is present (i.e., something you know). Furthermore, multiple people are likely to know your user ID as it is frequently nothing more than your social security number, e-mail address or something that follows a formula for everybody in the company (e.g., first initial separated by a period followed by the last name), so it does not provide an effective means of authentication. There are a variety of single-factor server products available today such as RADIUS and LDAP that store user names and passwords in a standard database format and provide other services such as accounting, but these are relatively insecure unless integrated with a stronger authentication system.

Traditional SSL VPN products are based on the premise that encrypting data during transit is more important than knowing who is on the end of a secured connection. They are not packaged with two-factor authentication systems and therefore lack the capability to authenticate end users. This model is usually acceptable for Internet based electronic commerce where credit cards are involved since the card issuer's bank normally provides protection in the event of fraud. In other words, a Web retailer like Amazon.com just needs a valid credit card number to process an order and does not need to be overly concerned with who is actually providing the card information since fraudulent use is largely the bank's problem. Contrast this to the damage caused by unauthorized access to sensitive information (e.g., engineering drawings or names of undercover law enforcement agents) where exposure can have serious financial impact or even loss of life.

In the world of electronic security, an access code, sometimes referred to as a "PIN," is defined as something entered into a data processing device for the purpose of verifying identity. It is normally used in conjunction with an authentication token, a physical object needed to access network services. A token usually takes the form of a small, easy-to-carry smart card, key fob or something similar, and serves as one of the two required elements in a two-factor authentication system.

Before moving on, take a moment to ask yourself if you would be comfortable protecting your personal bank account and assets with nothing more than a PIN code—that is, no associated physical card that provides a second factor of assurance. If you understand the risks and are like most people, the answer is "absolutely not!" The logical follow-on question then, is why would you ever want your corporation's information assets protected by a similar one-factor password-only approach?

AEP Networks Authentication

AEP Smartgate is a robust, enterprise class offering built upon industry and government standards, numerous U.S. patents, and over a decade of advanced research and development. This proven security solution includes a powerful two-factor authentication system packaged with the base offering at no additional cost, which is a significant distinguishing characteristic that sets AEP Smartgate apart from SSL and IPSec VPN offerings available today. Unlike other solutions, the strong authentication capabilities of AEP Smartgate were integrated into the product at the onset and are not add-ons that require separate integration or administration.

AEP solutions are based on the client/server paradigm depicted in Figure 2, where AEP SmartPass® client software connects to AEP Smartgate server software or an AEP SmartGuard appliance over an Internet Protocol (IP) based network. The IP transport mechanism can be terrestrial, satellite or wireless with virtually no impact on throughput or performance. AEP Smartgate acts as a "proxy" server in that it receives all SmartPass traffic through a single port for validation and processing before the traffic is routed to its ultimate destination, based on a set of administrator configurable rules. Among other responsibilities, AEP Smartgate acts like a traffic cop, allowing directed passage only to authorized traffic.

The AEP security solution integrates seamlessly into existing network infrastructures, co-exists with other devices including firewalls and VPNs, and can be used in complex, distributed architectures.

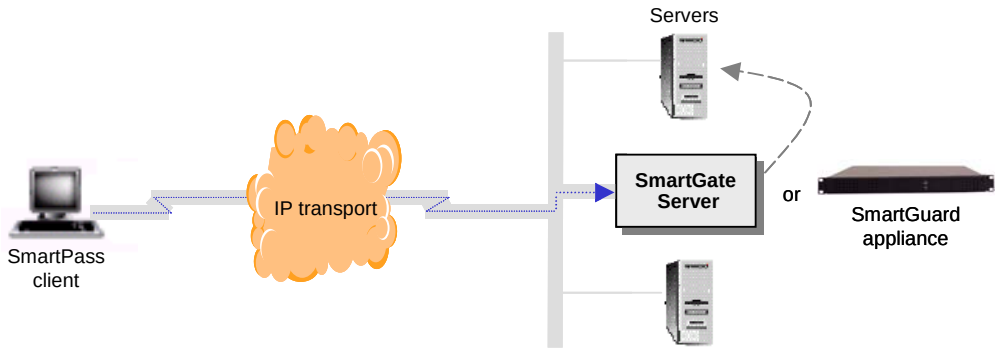

Figure 2: AEP Client/Server Security Model

AEP Smartgate employs two different authentication mechanisms to ensure that communication between an end user and destination can be trusted:

Mutual Authentication

Two-factor User Authentication

Mutual Authentication

Mutual authentication refers to the process of two-way, or mutual, verification between the AEP SmartPass client and AEP Smartgate server that is initiated upon activating SmartPass. At this stage, the AEP Smartgate server validates that the end user is legitimate, and, if successful, the client then verifies server identity. This reciprocated authentication procedure prevents spoofing, confirms that each entity is pointed to a legitimate location and ensures both the user and server can be trusted. The process is based upon a challenge/response algorithm using shared secret keys and is handled rapidly behind-the-scenes. Figure 3 depicts two-way identification checks that must be successful in order to proceed.

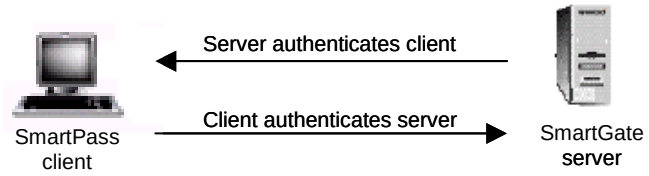

Figure 3: AEP Smartgate / SmartPass Mutual Authentication

User Authentication

AEP Smartgate has been designed around the concept of authenticating a *user*, not a device, making validation independent of the source IP address. This is a defining characteristic of AEP Smartgate and means a user can securely access information from almost any computing platform given the proper credentials—a valid access code and token combination—that form a digital identity and allow positive identification.

❶ ❷

Access code + Token ➡ Key to access

Access Code

Each user must possess and enter their own private access code when prompted by AEP SmartPass upon startup or after a timeout. The process is straightforward, relegated to simply typing a few characters into a text box, as shown in Figure 4, and resembles a typical password in that a string of alphanumeric characters is used. Access Code composition rules, validity period, a failed attempts counter and other parameters can be modified from default settings, if desired.

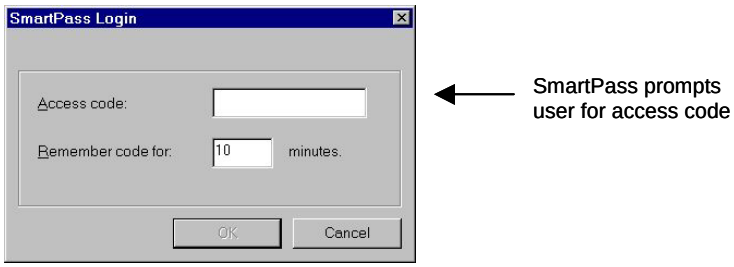

Figure 4: AEP SmartPass Access Code Entry

Though entering a string of characters into a SmartPass text box appears to be identical to the password process, there are significant differences and clear advantages to using access codes.

Entry of an Access Code into SmartPass represents only half of the credential package needed to authorize a user. It is the first component of a two-factor authentication system, not the sole means of validation.

Perhaps the most important differentiator between a SmartPass Access Code and a regular password is that a user's private credentials never transit a network for validation, unlike passwords. In fact, Access Codes are not stored anywhere and never leave the end user's computing device. The SmartPass Access Code is designed to "unlock" or "activate" a user's *local* token for use in the authentication process so other more secure and constantly changing information can be sent to the validation server. Lengthy computer-generated encryption keys are used during transmission that are almost impossible to crack in a timely manner even with automated utilities.

The fact that access codes are used locally without traversing a network is worth examining in greater detail. Consider the case of password transmittal in Figure 1 where an end user enters a user ID and secret password, submits, and then awaits an access permission or a failure message. Though the password is encrypted, the same password is repeatedly used over and over until it expires or is eventually changed by the user. In most cases, the life of a password is measured in months, sometimes years. In the event a password is captured, it can be used from any browser until the unauthorized activity is detected or the password is changed (even then, a hacker may have taken steps to position himself for future undetected access). Analysis shows that many people use the same or slightly modified passwords for most of their online activity, so a single compromised password can often be used as a starting point for opening many electronic gates.

Figure 5 depicts how AEP Smartgate avoids password transmittal problems by using an Access Code to unlock a user's private token which then starts the process of protecting transmitted data through the use of dynamic encryption session keys.

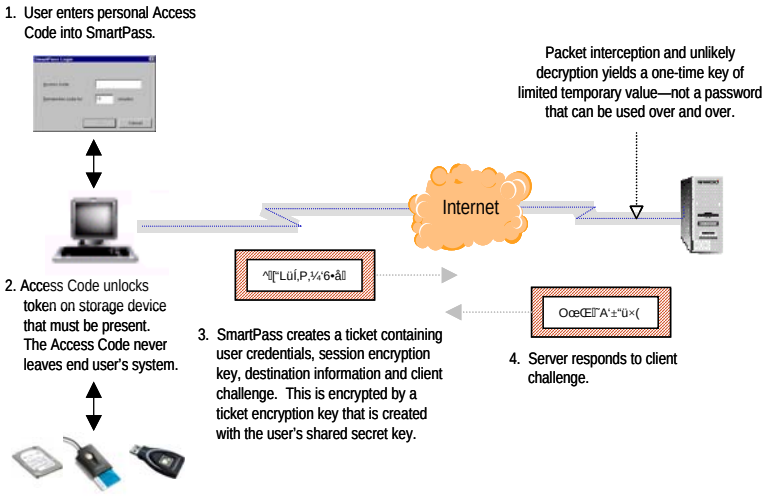

Figure 5: Access Codes are Never Transmitted Across a Network with AEP Smartgate

Today, both Microsoft Internet Explorer and Netscape Navigator browsers have the capability to retain passwords for automatic entry into a form when needed (see Figure 6). This convenient feature negates the need to re-enter passwords, but it obviously weakens security. Think for a moment about the potential damage of an unattended computer or stolen laptop PC with a collection of stored passwords that can be filled in automatically when an unauthorized person merely points the browser to a particular IP address. AEP SmartPass eliminates this problem by requiring a user to enter an access code that cannot be stored or looked up automatically. In fact, SmartPass will prompt the user to re-enter their code after a specified period of activity and/or inactivity, so damage is minimized even in the event an unauthorized user takes control of an unattended workstation. Other security features such as disabling connection attempts after a number of consecutive login failures can be enabled by an administrator.

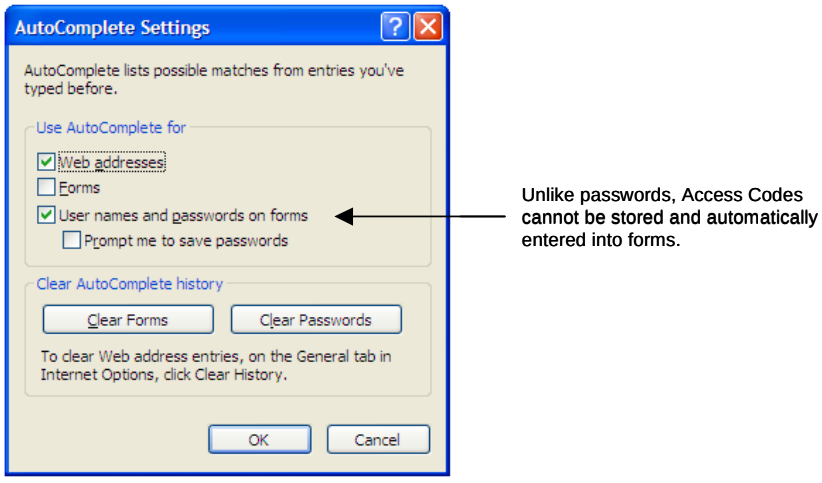

Figure 6: Browser Password Retention and Automatic Form Completion

AEP Smartgate was designed so that private access codes are generated by and only known to individual end users. Nobody else—not even the root level system administrator—can obtain this information. Since users select their own code, subject to

format constraints like minimum length, there is a far less likelihood of forgetting the string and needing to contact a support desk for assistance. It is normal for password-related call volume to an IT support desk to drop dramatically once a AEP Smartgate system is deployed. As mentioned, every call for assistance has a cost that can multiply quickly, especially when the community size is large.

Authentication Token

AEP Smartgate comes packaged with an integrated two-factor authentication system that includes a virtual "soft" token. A soft token is software emulation of a physical hardware token used to store the encrypted authentication key. Since the token and access code are portable, a user is not locked to a specific device. The AEP token is validated for U.S. Government use since it adheres to FIPS 140-1 cryptographic module implementation standards set forth by the National Institute of Standards and Technology (NIST). Having this designation is significant and the reason why AEP's token is frequently referred to as a "FIPS token" or "FIPS validated token."

AEP Smartgate can store the user's private encrypted authentication key in a variety of locations including the user's hard disk or removable floppy drive, USB Thumbdrive, smart card, biometrics smart card (e.g., a fingerprint reader) and a variety of other generic and third-party token storage devices. In its simplest form, a soft token can be stored on a user's hard disk drive and looked up automatically when the Access Code is entered.

Figure 7 illustrates some of the token storage devices that can be used with AEP Smartgate, all of which have considerations like convenience, cost and level of security.

Three-Factor Authentication

Moving from a two-factor authentication model to a three-factor approach, which AEP Smartgate supports, further enhances security. An accepted definition for the third factor is "something you *are*," which translates to biometric information commonly obtained from unique things such as finger or handprints, retina or iris scans, face identifiers, hand geometry or a voiceprint. Small inexpensive thumbprint biometrics devices are available today that can store a token and be plugged into a computer's USB port.
Using a three-factor approach means a user is required to possess three valid items to access a protected system:

1. Physical token
2. Access code
3. Biometrics information

Even if a physical token is lost or stolen, it is worthless unless the new holder can reproduce stored biometrics information (e.g., a thumbprint) and obtain the valid access code.

Figure 7. AEP Smartgate Works with a Variety of Token Storage Devices.

Possessing separate user ID/password pairs for more than a couple of accounts can be difficult to memorize, cumbersome to manage, and increases security concerns. In practice, most computer users have access to multiple accounts, for personal and business purposes. Information being accessed is often distributed among various systems and locations, and under the administrative control of different departments, business units or even external organizations.

The need for users to remember and manage multiple user ID / passwords combinations can be minimized or eliminated with a powerful capability in AEP software known as AEP Smartgate Aware™. Coupled with AEP Smartgate authentication and fine-grained access control protection measures, users only need to be authenticated by AEP Smartgate prior to being routed and permitted to access applications and resources specified by the system administrator. User credentials are automatically passed to designated applications without further end user interaction, thereby providing a "single sign-on" capability. This means after being authenticated by AEP Smartgate, users can access their e-mail and company intranet, for example, without needing to separately log on to each system.

AEP Smartgate allows separation of the encryption and authentication servers to cost effectively enable "single sign-on" access to information resources managed by multiple entities. In this model, a user's Access Code and token can be used to authenticate with multiple AEP Smartgate servers. Figure 8 depicts a configuration in which a single user can access information managed and controlled by various organizations.

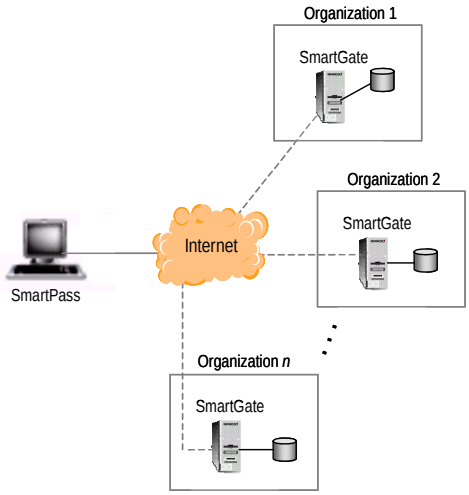

Figure 8. Users Register Online to Receive Their Personal Authentication Token.

Token Distribution & Registration

AEP Smartgate includes an innovative, patented On-line Registration (OLR) capability that allows even non-technical end users to enroll from their browser and begin accessing secured applications in minutes. Software download, token distribution, registration and activation of an end user's account can be handled entirely online in a secure manner using advanced technology. In sharp contrast to other products and problems associated with ramping a community, this is a painless process that has been repeatedly used to deploy thousands of users in very short time frames. Due to the simplicity of this process, no IT help desk support, software driver adjustments or network configuration changes are needed.
To be enabled a new user simply:

Downloads "lightweight" SmartPass software and installs via an easy-to-use wizard.

Chooses a personal Access Code and generates random data through mouse movement.

Provides information required by the administrator into an enrollment form (see Figure 9).

Awaits administrative approval and then begins using the activated account to securely access information.

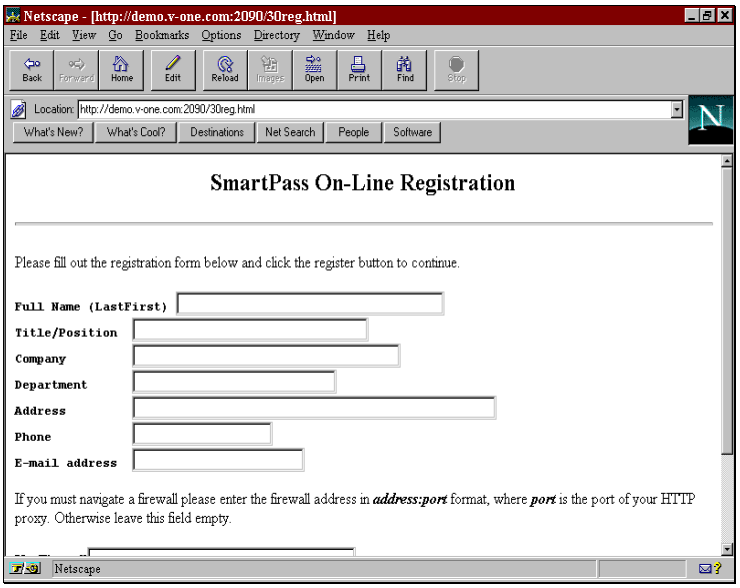

Figure 9: Users Register Online to Receive Their Personal Authentication Token

Though this process is straightforward and not much more complex than completing an online form and following basic instructions, beneath the surface interaction between the client and server of an entirely different nature is taking place. A two-way process involving public/private, session, and shared secret cryptographic keys are used in the key distribution and activation process. The technical details are quite interesting, but outside the scope of this paper.

The ease with which end users can be deployed and fitted with two-factor or greater user authentication is a distinguishing characteristic of the AEP solution. This approach should not be confused with the simplicity of which many SSL VPN solutions and other security products handle *one-factor* password security. AEP Smartgate excels at quickly ramping extranet communities, where end user desktops belong to another organization, due in part to its ability to take advantage of already-open firewall ports and avoidance of network address translation issues.

Beneath the Surface

After the initial launch of AEP SmartPass, a unique authentication key is generated. This encrypted key is stored on the user's token storage device (which could be their hard drive) and in the AEP Smartgate server user database. When the AEP SmartPass client prompts a user to enter their Access Code, the identification and authentication process begins. The technical details involve complex mathematics and algorithms, so only an abbreviated high-level overview is presented.

AEP SmartPass first opens a TCP connection and prepares a "ticket" that contains all the data required for authentication. The ticket is encrypted with a single-use Ticket Encryption Key (TEK), that is created by the user's shared secret key. User credentials, TEK, destination information and the ticket (but not the Access Code) are then sent as a package to the AEP Smartgate server. When the server receives this data, it retrieves the user's shared secret key, decrypts the TEK, and then decrypts the ticket itself. The server then processes the service request and responds to the client challenge. Each client TCP connection generates a new authentication ticket and has a unique session key.

When the AEP SmartPass client is launched, it automatically contacts every AEP Smartgate server with which the user has registered and requests current access permissions using a standard AEP Smartgate secured session. Access permissions are created and controlled by the AEP Smartgate administrator. AEP Smartgate server(s) return the user's current access permissions to the SmartPass client. The user's access permissions are dynamically updated at startup and at regular intervals and never stored in permanent storage on the client's system. Every encrypted session, as well as the identification-

authentication-dynamic configuration sequence occurs within seconds. During the transmission of encrypted data, an end user will notice a small gold lock appearing over the SmartPass icon in the taskbar, as shown on the right.

AEP Smartgate Security Features

AEP Smartgate contains a plethora of security features that can be grouped into the following general categories: encryption, access control, management and control and auditing/logging.

Encryption – Dynamic encryption keys are used to ensure that user data and sensitive addressing information is never transmitted in the clear. Highly efficient FIPS validated AES (128, 192 or 256-bit) and 3DES (3 x 56 bit) protection is available. Constantly changing session keys ensure only a limited amount of information is transmitted with a specific encryption key, reducing risk.

Access Control – The AEP Smartgate server determines if an access request is legitimate, and if so, routes the traffic to the appropriate destination based on an administrator-defined access control list. Users and/or groups can be given passage rights to an entire network, set of applications or even a single URL through "fine-grained" access control mechanisms.

Management & Control – SmartAdmin™ is a powerful Web-based administrative tool that allows remote, centralized or distributed management of users, groups and access control lists. There are five levels of administrative privileges ranging from superuser to view-only access of limited information. Figure 10 provides a snapshot of a SmartAdmin access list permission screen.

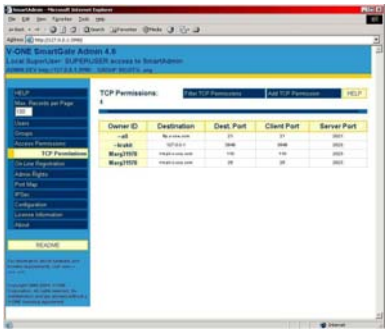

Figure 10: SmartAdmin Allows Secure Web-based Management & Control of Users and Groups

Auditing & Logging – Event data is logged continuously and automatically during all SmartPass-to-AEP Smartgate interaction. This data can be reviewed periodically, if attempted intrusion is suspected, or passed along for formatting and reporting. Several filter levels are available that regulate the amount and type of data that is captured.

Validation and Compliance

When dealing with computer security, it is essential that a system using cryptographic algorithms and modules be certified by a reputable third-party to ensure conformance to security standards and the ability to pass a comprehensive series of tests. The "trust us" approach or mentality that one can just rely upon big-name companies does not work when dealing with matters of this nature.

AEP Smartgate has successfully passed numerous formal testing programs over the years (e.g., ICSA Labs) and is currently FIPS 140-2 validated, one of the most in-depth and respected security assessments available today.

Federal Information Processing Standard (FIPS) 140

AEP Smartgate encryption and authentication modules are FIPS validated. Validation testing and documentation is a time-consuming, intensive, and thorough procedure that is conducted by a certified test laboratory.

The FIPS 140 U.S. Government standard specifies security requirements to protect sensitive data that must be met by every Federal organization using cryptographic-based computer and/or telecommunication systems. The standard was created by the National Institute of Standards and Technology (NIST) and specifies requirements related to the design and implementation of cryptographic modules that include:

Authentication	Module ports and interfaces
Authorized roles and services	Operational environment
Design assurance and documentation	Operating system security
Cryptographic module specification	Physical security
Key Management	Self-tests
Mitigation of attacks	Software security

Having the FIPS credential means AEP Smartgate has been approved for use in the U.S. Government and is independently verified to meet all published requirements. This credential is also assurance to those in the commercial sector that AEP Smartgate has passed all tests necessary to handle and transmit sensitive information.

Regulatory Compliance

There are an increasing number of government regulations and industry guidelines in place or being developed to ensure privacy, control access, and allow auditing of electronic information. AEP Smartgate has been designed to meet stringent security requirements and is compliant with the following legislation:

Gramm-Leach-Bliley Act – Enacted by the U.S. Office of the Comptroller of the Currency (OCC), it requires financial institutions to regularly review and update security controls including authentication, access control and encryption.

HIPAA – The Health Insurance Portability & Accountability Act mandated by the U.S. Department of Health and Human Services (HHS) sets standards for the electronic access, transmittal and disclosure of healthcare related information.

Sarbanes-Oxley Act – A directive of the Security and Exchange Commission (SEC) aimed at improving corporate accountability for companies publicly traded on a U.S. exchange. It legislates acceptable conduct and establishes new standards for processes related to financial reporting.

21 CFR Part 11 – U.S. Food & Drug Administration (FDA) guidelines and requirements for pharmaceuticals and other FDA regulated companies concerning authenticity, integrity and confidentiality, where appropriate, of electronic records.

Conclusion

VPN products available today are geared toward encrypting data between two points and providing only rudimentary one-factor password protection—insufficient to authenticate the identity of end users. Passwords can be relatively easy to guess or crack with automated tools, are deceivingly expensive to support and represent a security risk when transmitted across a network for validation. Given that passwords have numerous shortcomings and limitations, organizations must question whether the ongoing risks and costs associated with password use are acceptable.

AEP Smartgate addresses the password problem by providing an integrated FIPS 140-1 validated, two-factor user authentication system as part of the standard offering. Three-factor protection is available through the use of optional

biometrics token storage devices. By requiring a user to possess a private SmartPass Access Code and personal soft token, that can reside on a wide range of storage devices, users are identified and authenticated before their data is safely transported across a network. AEP Smartgate does not transmit sensitive user or addressing information in the clear and never permits a user's private access code to transit a network.

AEP Smartgate offers a wealth of security features and functionality including a patented, user-friendly, online token distribution and registration system that makes deployment of large intra/extranet communities simple and fast. 256-bit AES encryption with dynamic session keys, fine-grained access control capabilities that can restrict passage to a sole URL, single sign-on accessibility and much more comes standard with the offering.

AEP Network solutions are validated for use in the U.S. government and meet requirements set forth by various federal and industry regulations.

Why AEP Networks?

Complete Security Solution – U.S. Government FIPS 140-1 validated strong multi-factor user authentication system for better than password-only protection, end-to-end AES encryption, fine-grained access control and powerful administrative capabilities.

Easy Implementation and Use – Solutions integrate seamlessly into existing network infrastructures and do not interfere with already installed firewalls and VPNs. Rapid deployment of user communities, including extranets, minimizes total cost of ownership.

High Performance Wireless VPN – Patented technology is engineered to work efficiently over IP based satellite, wireless and terrestrial networks with virtually no impact on performance. Throughput gains over satellite circuits in excess of 10:1 versus other VPNs are typical.

Proven Track Record – AEP Networks has over 10 years experience in large government and global corporate environments. Solutions are used by numerous Global 1000 companies and large federal agencies.

Contact AEP Networks

Corporate Headquarters	Government Solutions Group
AEP Networks 347 Elizabeth Ave., Suite 100 Somerset NJ 08873 Toll-Free: 1-877-638-4552 Tel: +1 732-652-5200	AEP Networks 40 West Gude Drive, Suite 200 Rockville, MD 20850 Toll-Free: 1-800-495-8663 Tel: +1 240-399-1200
Europe	**Asia-Pacific**
AEP Networks Focus 31, West Wing, Cleveland Road Hemel Hempstead Herts HP2 7BW U.K. Tel: +44 1442 458 600	AEP Networks 2107 Tower 2 Lippo Centre 89 Queensway Hong Kong Tel: +852 2845 1118
Japan	
JOYO Bldg 6-22-6 Shimbashi Minato-ku Tokyo 105-0004 Japan Tel: 81-3-3432-3336	

APPENDIX

AEP Networks Authentication Patents

High-level summaries of two patents belonging to AEP Networks are listed below, both of which use innovative technology in combination with proven open standards.

United States Patent 6,061,796
Multi-access Virtual Private Network
AEP Networks
Filed: August 26, 1997
Effective: May 9, 2000

A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program and at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computer to intercept function calls, requests for service, or data packets in order to communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer-to-peer applications, the intercepted function calls, requests for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications.

United States Patent 5,784,463
Token distribution, registration, and dynamic configuration of user entitlement for an application level security system and method

AEP Networks
Filed: December 4, 1996
Effective: July 21, 1998
A shared secret key distribution system which enables secure on-line registration for services provided by an application server through an application level security system or firewall utilizes an authentication token containing a server public key. The server public key is used to encrypt a client-generated portion of the shared secret key, and the encrypted client-generated key is sent to the server where it is recovered using a private key held by the server and combined with a server generated portion of the shared secret key to form the shared secret key. The server generated portion of the shared secret key is then encrypted by the client-generated portion of the shared secret key and transmitted to the client for recovery and combination with the client-generated portion of the shared secret key, at which time both the client and server are in possession of the shared secret key, which can then be used for mutual authentication and development of session keys to secure subsequent communications. The session keys can be used to provide dynamic configuration of a client system to provide for different or changing user entitlements.