Virtual Private Networks for the Health Care Industry

SmartGate Conformance to the HCFA Internet Security Policy

February 1999

Executive Summary

With government mandates to do more with less, the health care industry is looking at alternatives to private networks. The on-going operating costs of purely private networks seem to increase with every advancement in technology. There are more users demanding to be "on-line"—around the clock and around the globe. New applications consume ever-increasing amounts of bandwidth. And the many so-called legacy applications must continue to exist in harmony with new browser-based ones.

As a result of the increasing complexity—and cost—of private networks, many organizations are turning to Virtual Private Networks. A VPN is a "private" network application that utilizes the Internet as a wide area network (WAN) backbone. Because all connections to the Internet-based VPN are local, long-distance dialup and leased line charges (the single largest operating cost of private networks) can be eliminated. Analysts predict—and users report—that VPNs can cut remote networking costs in half.

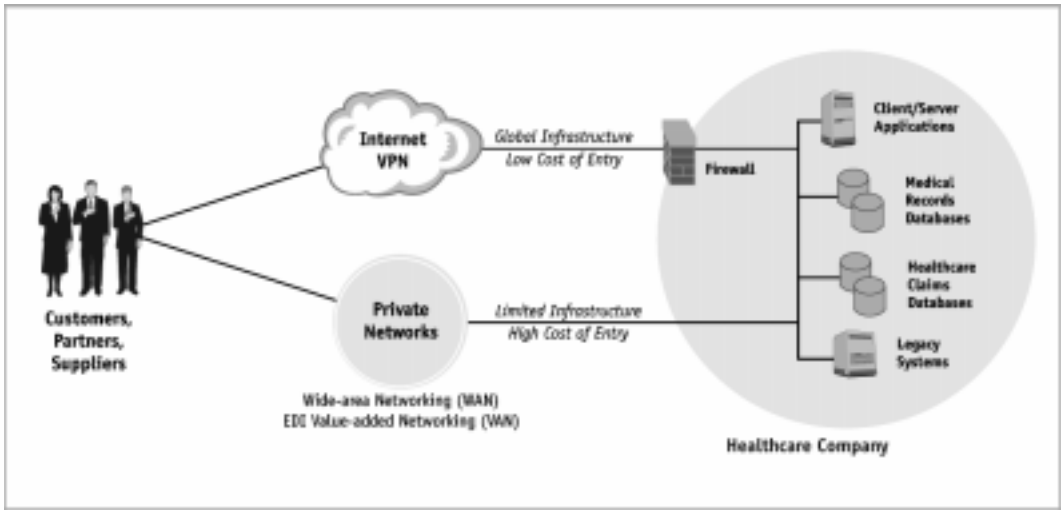
Advantages of an Internet-based VPN

- Lower networking costs—from 30 to 80%
- Extend reach worldwide—with local access
- Improve productivity easily and affordably
- Achieve high reliability with the redundancy and resiliency of the Internet
- Increase flexibility and simplify operations with a single per-site connection to an intranet, extranet(s) and the Internet
- Leverage enhanced and expanded services that are unavailable in the Public Switched Telephone Network (PSTN), such as IP Multicast
- Take advantage of the proven interoperability of IP-based applications, especially the powerful user-friendly Web browser

Until recently, patient record and other security issues have prevented widespread adoption of VPNs in health care applications. But new guidelines published by the Health Care Financing Administration (HCFA) establish the first set of definitive security standards covering sensitive health care information. The Health Insurance Portability and Accountability Act (HIPPA) will build on HCFA's ground-breaking work, bringing the full benefit of cost-saving VPN technology to the health care industry. In fact, with the robust security provisions now available for VPNs, the typical VPN is actually more secure than the typical private health care network.

The most anticipated VPN application for health care is the “extranet.” An extranet is network among multiple, independent parties; examples include doctors accessing patient records and Medicare claims processing. In addition, many organizations might benefit from “intranets” among their own staff and offices. Examples of intranets include hospital staff accessing patient records from their homes or offices, outpost clinics communicating with the main hospital, and insurance companies creating an internetwork of sales offices.

Indeed, VPNs will allow patients, doctors, medical organizations, insurance companies and government agencies alike to communicate effectively and economically—and securely—in this exciting new dimension of truly modern medicine.



A VPN improves productivity and extends reach with a more affordable, capable, flexible and secure alternative to the typical private network.

This white paper provides an overview of VPN security considerations, including HCFA policy requirements, and describes how SmartGate® from V-ONE® conforms to these comprehensive requirements. Additional information on various aspects of VPN security is available at V-ONE’s Web site (www.v-one.com).

VPN Security Considerations

The Internet was designed as an open network with virtually no security built-in. Such an open design helps explain the Internet's unprecedented popularity and growth, but it also undermines other potential (and unforeseen) uses—such as VPNs. Ironically, the very openness that makes the Internet pervasive also makes it ideal for private inter- and intra-organizational communications.

Fortunately, the Internet is not incompatible with security. In other words, robust security provisions can be added quite easily to Internet access and/or the many IP-based applications. The fundamental security provisions required for an Internet-based VPN are easily remembered as the three P's of network security:

- Protection of resources
- Proof of identity
- Privacy of information

Protection of resources is provided by the firewall. Firewalls screen all inbound and outbound traffic to grant only trusted users access only to authorized applications. Determining who is a trusted user (proof of identity) is the role of authentication. Authentication systems positively identify all legitimate or trusted users, all of who must be registered in a database, which is itself secured. Finally, information is made private with both encryption and authorization. Encryption protects privacy while the information is in transit; authorization or access control protects the information in its stored form on servers or host systems.

HCFA's Internet Security Policy

The Health Care Financing Administration's Internet Security Policy outlines specific requirements for VPN security. HCFA's policy satisfies the demanding Privacy Act of 1974, which requires that federal information systems protect the confidentiality of individually-identifiable data. As such, the policy is expected to serve as the foundation for future efforts involving VPN-based applications for the health care industry.

> "It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information."
>
> -- HCFA Internet Security Policy

HCFA specifications conform to the three P's of VPN security. "Technologies that allow users to prove they are who they say they are [proof of identity] (authentication or identification) and the organized scrambling of data [privacy of information] (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties."

Firewalls [protection of resources] are recognized as being essential in the HCFA policy, but are not addressed in detail: "Local site networks must also be protected against attack and penetration from the Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document."

The policy outlines specific requirements in three areas: encryption, authentication and identification.

Encryption specifications permit three alternatives or their equivalents:

- Triple DES (defined as 112-bit equivalent) for symmetric encryption,
- 1024-bit algorithms for asymmetric encryption, or
- 160-bit elliptical curve forms of encryption.

Authentication, which must occur at the beginning of each session, is permitted using one of four methods:

- locally-managed digital certificates, providing all parties are covered,
- use of third-party certificate authorities,
- self-authentication as an internal control of private keys, or
- tokens or “smart cards”.

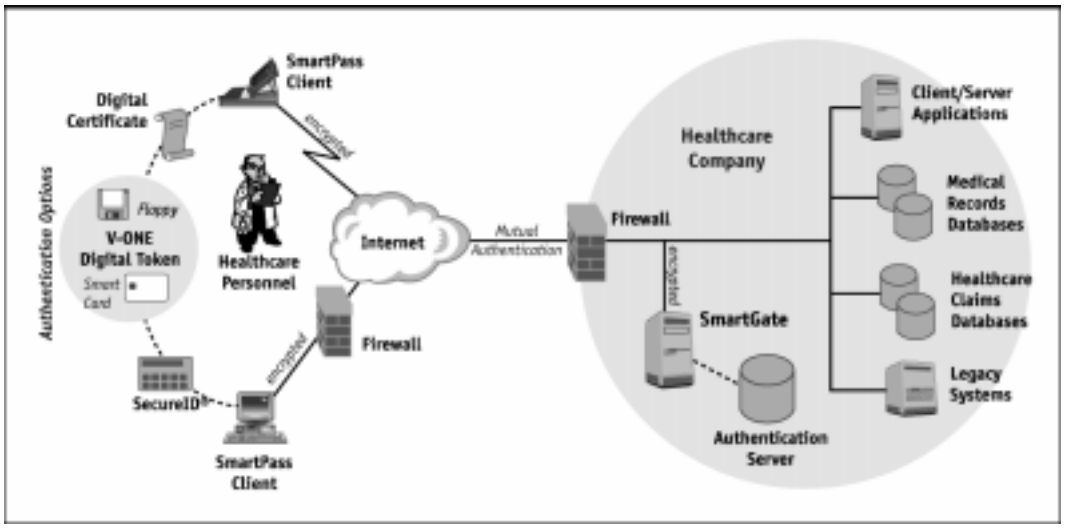
Identification of users, which may involve exchange of passwords, is a one-time task that occurs when users establish the extranet account. Four “out of band” and one network-based approach are approved. The old-fashioned out-of-band methods are by telephone, certified mail, bonded messenger or direct personal contact. The more modern approach is to use tokens or smart cards.

Note that tokens or “smart cards” are permitted for both the initial identification of users and their on-going authentication. These “two-factor” security systems are far superior because all users are authenticated based on something they have (the token or smart card) and something they know (an access code or personal identification number). Tokens are generally implemented in software; a smart card is, in effect, a physical token that resembles a credit card.

V-ONE's Comprehensive SmartGate VPN Solution

SmartGate integrates encryption, authentication, authorization, accounting and access control into a complete, compatible and affordable software-based VPN solution.

Its comprehensive nature has made SmartGate the Federal Government's preferred solution for end-to-end, application-level VPN security. SmartGate provides a total solution that both protects the privacy of information and ensures the integrity of electronic transactions. In addition, V-ONE supports the Defense Messaging System and is certified compliant with FIPS 140-1. Among V-ONE's many Federal Government users are the Centers for Disease Control (CDC), the departments of Defense, State and Treasury, and even the demanding National Security Agency.



SmartGate provides a complete and highly compatible and affordable software-based solution for HCFA-conformant Internet-based VPNs.

The SmartGate solution has two components: the SmartGate Server and the SmartPass® Client. The SmartGate Server manages and monitors user authentication and access privileges, ensuring that only trusted users are accessing only authorized resources. The server has an integrated user database, or it can utilize third-party databases, such as RADIUS (the Remote Access Dial-In User Service) and ACE for support of Security Dynamics' SecurID® token.

The SmartPass Client provides a user-friendly, wizard-guided interface for two-factor authentication with the SmartGate server. The SmartPass Client supports V-ONE's own software-based tokens and most third-party smart cards, as well as third-party certificate authorities. V-ONE's authentication is also two-way, or mutual. In other words, the system authenticates both the SmartPass Client end and the SmartGate Server end of the VPN to give all parties confidence in the session.

SmartGate Conformance to HCFA's Internet Security Policy

SmartGate meets all three provisions of HCFA's Internet Security Policy:

- Encryption – SmartGate offers a choice of encryption options, including the Triple Data Encryption Standard (3DES) implemented with three 56-bit keys.
- Authentication – SmartGate's two-factor mutual authentication goes well beyond the minimal requirements established by the HCFA, supporting all four methods permitted under the policy.
- Identification – SmartGate supports both the built-in SmartPass client token and popular third-party smart cards. SmartGate is, of course, also compatible with the four out-of-band procedures specified.

Together the SmartGate Server and SmartPass Clients permit (and restrict) user access to specific applications on a real-time, dynamic basis, and any session can employ one of the many built-in encryption options.

SmartGate and SmartPass integrate seamlessly with existing firewalls, and are available with V-ONE's own SmartWall® firewall. SmartWall is optimized for VPNs with features like IPSec compliance, application-level proxies, NCSA (National Computer Security Association) certification, and activity logging and reporting.

SmartGate's unique On-Line Registration (OLR) provides numerous advantages, including ease of use, configuration flexibility and low operating costs. Users can download the SmartPass client on-line—with the built-in token—or the software can be distributed on diskettes as part of an out-of-band identification process. The client set-up procedure is so simple and straightforward that even novice users are up and running within minutes. Once users have been identified and authenticated at the beginning of each session, the SmartGate Server and SmartPass Clients

The SmartGate Advantage

- Delivers unparalleled ease of use, especially for SmartPass client users
- Dynamic, on-line enrollment with SmartPass makes it easy to add new users
- The common SmartPass client (Windows and Macintosh) assures interoperability and provides for conforming authentication through digital certificates
- Virtually unlimited scalability makes SmartGate capable of supporting several hundred thousand users
- Access control provides authorization by application, host/server, port or URL
- The event log helps detect attempted security violations, affords a means of extranet accounting, and helps establish HCFA conformance during an audit
- Integrates seamlessly with existing firewalls, internetworking equipment and authentication databases, such as RADIUS or SecurID/ACE
- Imposes minimal maintenance requirements on IT personnel
- Operates on a wide variety of cost-effective UNIX systems
- Works with popular third party "smart cards" and Certificate Authorities
- Offers compatibility with the emerging Public Key Infrastructure (PKI)
- Available with optional SmartWall firewall

automatically exchange encryption keys to ensure strict privacy across the VPN. The SmartGate Server, as configured by the network manager, then monitors traffic constantly to enforce access control, or user entitlements, thereby assuring that only authenticated users are accessing only authorized resources.

Just as importantly, the SmartGate solution is also low maintenance with full and friendly GUI-based control over user access from a common database at a single, secure location. And the relatively simple SmartPass client minimizes the need for user training and remote support. One real time-saver, for example, is the non-intrusive nature of SmartPass on the desktop, which makes it unnecessary to alter WINSOCK files—an error-prone process that frequently causes problems in other VPN security solutions.

V-ONE's SmartGate affords health care users two major advantages: compatibility and ease of use. Its highly compatible design satisfies the dilemma of being "open" enough for interoperability in the inherently heterogeneous environment of extranets, while still maintaining iron-clad security. SmartGate's hardware-independent, software-independent operation is compatible with the existing network infrastructure, which maximizes investment protection. Seamless integration is virtually assured with SmartGate's single-port transversal of firewalls, which utilizes proven Secure Sockets Layer technology. And it works with or without the emerging Public Key Infrastructure (PKI), making SmartGate a long-term solution that overcomes all short-term obstacles.

SmartGate's second major advantage is its remarkable ease of installation and use, especially for all clients, including relatively unsophisticated patients. A simple

wizard guides the user through a short installation process. The client's non-intrusive design makes it unnecessary to interface with special drivers or alter any existing files. And once installed, SmartGate's unique On-Line Registration (OLR) system delivers simple yet dependable operation.

For today's demanding network security needs, no other solution is as capable, flexible and affordable as V-ONE's field-proven SmartGate/SmartPass combination.