

Go Secure!SM

for Virtual Private Networks

Secure your VPNs—virtually overnight

Virtual Private Networks (VPNs) based on IPSec let you cost-effectively extend your intranet to connect remote users, offices, partners, and customers via the Internet. But business-critical information transmitted via VPNs is vulnerable to hackers, and some security solutions are either inadequate or too difficult to scale for large enterprises. Ensure the confidentiality and integrity of your VPN and authenticate the identities of its users—rely on the VeriSign OnSiteSM managed service. OnSite lets you issue IPSec digital certificates to every client and device (including firewalls, routers, and servers) on your VPN, without proprietary hardware and software or time-consuming training and maintenance. And with the new Go Secure! service for Virtual Private Networks, you can integrate digital certificate security into your VPN quickly and easily while staying focused on your business instead of on building a new security infrastructure.

IPSec: The standard for secure VPNs

Internet Protocol Security Standard (IPSec) secures private communications on the Internet at the network level between firewalls, routers, and remote access devices. IPSec authenticates the identities of communicating parties, protects data from alteration, and safeguards information from interception using packet formats, and because it encrypts only “payload” information, leaving network-level headers in the clear, IPSec is transparent to intermediary network layer devices. The Internet Key Exchange (IKE), part of the information transmission process, authenticates each side of an IPSec transaction and creates a secure path for encrypted data packets to travel to their destination on the network. But for identity authentication to take place, every VPN device requires a digital certificate.

Digital certificates and PKI: Essential elements of VPN security

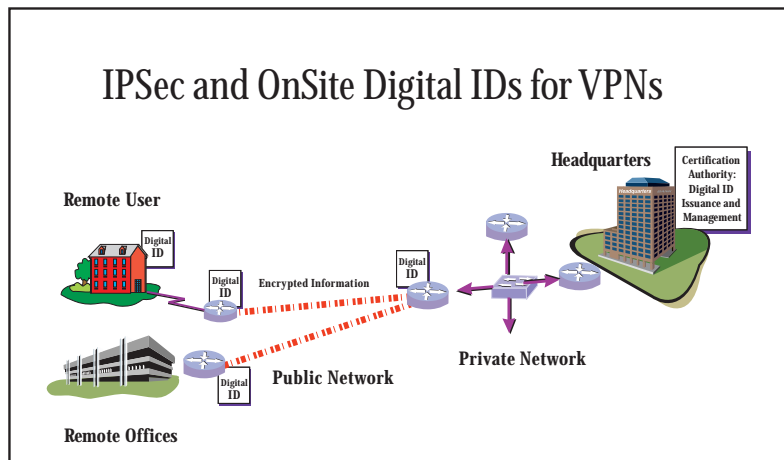
IPSec can use either “shared secret” keys or Public Key Infrastructure (PKI) Keys to encrypt data—but shared secret keys can’t scale beyond a handful of devices. VeriSign’s OnSite managed service is the ideal solution for efficiently issuing IPSec Digital IDs with PKI Keys to every VPN device in your enterprise. Easy-to-use-tools let your administrator control the approval, enrollment, validation, issuance, and renewal of Digital IDs while relying on VeriSign’s certificate processing, back up, key recovery, and customer support services. End users interact with customized, Web-based enrollment forms to request IDs for IPSec devices. OnSite can be scaled to accommodate even the largest IPSec networks. And all without requiring you to invest in proprietary software and additional hardware; a complex, secure back-up infrastructure; or time-consuming training and maintenance.

Key Benefits

- **Fast and easy to deploy:** Go Secure! for Virtual Private Networks helps you secure your VPN with digital certificates virtually overnight, without changing your IT infrastructure. The step-by-step Implementation Guide walks administrators through the entire deployment process, and a variety of special programs and services offer you access to expert assistance from VeriSign.
- **Fast and easy to use:** The OnSite Control Center provides intuitive tools for managing Digital IDs, and Go Secure! helps you automate certificate acquisition and authentication.
- **Scalable:** The OnSite service, together with Go Secure!, grows with your enterprise, issuing as many digital certificates as you need without requiring incremental investments in hardware, database administration, customer support, or physical security.
- **Reliability:** VeriSign’s high-security Operations Center provides certificate processing, back-up systems, key recovery, and 24x7 customer support.
- **No hardware and software required:** All you need is a Web browser (Netscape® Navigator™ or Netscape Communicator™, or Microsoft® Internet Explorer), Internet access, and IPSec-compliant products, like those from leading vendors Check Point, Cisco, IRE, and Network Associates.



IPSec and OnSite Digital IDs for VPNs



About Go Secure! services

Go Secure! for Virtual Private Networks is part of a revolutionary new suite of managed services designed to dramatically accelerate the way enterprises secure mission-critical applications for intranets, extranets, Web sites, and networks. Go Secure! services plug into your existing IT infrastructure without requiring you to change your network or desktops, and together with VeriSign OnSite digital certificate services, give you everything you need to quickly incorporate digital certificate-based security into your applications. Other Go Secure! services include Go Secure! for Microsoft Exchange, for securing enterprise e-mail messaging, and Go Secure! for Web Applications, for securing intranet and extranet enterprise applications for such uses as ERP, supply chain management, and e-banking.

Components of Go Secure! for Virtual Private Networks

- Automated certificate acquisition—Go Secure! integrates with existing remote access clients from providers such as Check Point, Cisco, IRE, and NAI and supports automated enrollment protocols such as CEP to automatically request and receive certificate management services from VeriSign.
- Automated authentication—Go Secure! includes the OnSite Passcode Authentication System, which automates approval of certificate requests without any local programming or database management.
- Administrator handbook—Go Secure! includes an easy-to-use Implementation Guide and tailored support services.
- Discovery Needs Assessment—Go Secure! provides access to VeriSign experts who help you devise a VPN security solution, including an architecture plan, component vendor recommendations, and a pilot-ready VPN Deployment Plan.
- QuickStart Services—This bundled software and services solution allows you to deploy OnSite for 100 users. VeriSign experts help you select, pilot, test, and deploy a VPN, install and integrate vendor gateway and client products, and train your IT staff.
- Enterprise VPN Deployment Services—Building on QuickStart, Deployment Services help you with large-scale VPN deployments. VeriSign experts install and integrate products and operate the system until it's ready to hand off to your administrators.

“VeriSign OnSite

works with Cisco IOS software to deliver critical security needs, making the deployment of networking security features more practical, cost-effective, and secure than ever before.”

- Roger Farnsworth
Manager, Security Internet Services
Cisco Systems

System Requirements

- Administrator's Kit, which comes with your purchase of OnSite, including a stand-alone Smart Card reader and card, and necessary installation software
- Netscape Navigator 4.0 or later or Microsoft Internet Explorer 4.0 or later, for obtaining Administrator's Certificate
- Microsoft Window 95 or Windows NT®
- End users need access to the Internet and firewall or router devices

For More Information

For more information about VeriSign OnSite and Go Secure! services or for a free test-drive of OnSite, visit www.verisign.com. To contact a VeriSign Sales Representative, call 650-429-5115, or send an e-mail message to verisales@verisign.com.



1350 Charleston Road • Mountain View, CA 94043
phone 650.961.7500 • fax 650.961.7300
www.verisign.com

© 1999 VeriSign, Inc. All rights reserved. VeriSign is a registered trademark exclusively licensed to VeriSign, Inc. OnSite and Go Secure! are service marks of VeriSign, Inc. Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft, Inc. in the U.S. and/or other countries. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. All other trademarks are properties of their respective owners.