



DATA SHEET



KEY BENEFITS

Minimize risk of unauthorized access

Cost-effectively deploy secure remote access to employees, contractors, and partners.

Reduce total cost of ownership (TCO)

Leverage VeriSign managed services and global infrastructure to reduce TCO.

Deploy scalable architecture

Establish unified security architecture for multiple access methods, including remote access and wireless local area networks.

Comprehensive Security for Enterprise Remote Access

Network communications and application access among distributed employees and applications has become critical to the daily operation of most enterprises. Networks span broad geographies to support email, Web-based applications, supply chain and financial systems, and other fundamental corporate computing needs. Securing and protecting these networks, as well as the information that flows over them, has become increasingly important.

In particular, enterprises need a coordinated response to several challenges: securing access to networks and services from outside the enterprise network boundary, protecting data as it travels over public networks, and managing, monitoring, and protecting the devices that comprise a virtual private network (VPN).

VeriSign offers a suite of services to enable enterprises to deploy secure remote access to their global user base:

- **VeriSign® Unified Authentication**—Enables enterprises to leverage existing infrastructure for authenticating a variety of digital credentials—including digital certificates, dynamic one-time passwords, and USB tokens with smart card technology—to minimize, if not eliminate, unauthorized access, while reducing costs.
- **VeriSign® Managed Security Services (MSS)**—Helps ensure 24/7 uptime and effectiveness of the enterprise's global VPN infrastructure.
- **VeriSign® Consulting Services**—Enables enterprises to design and implement a cost-effective and scalable architecture for secure remote access.

+ Security Architecture for Network Access

Many enterprises are discovering that their security architecture for network access has not kept up with growth in user demand and the evolution of network access technologies. With the rapid increase in home broadband connections—teleworkers, mobile employees, and contractors—remote access has evolved from a tool used by a few select employees to a must-have requirement for a majority of enterprise users. At the same time, network-access technology has evolved dramatically. The popularity of wireless local area networks (WLANs), or wireless LANs, for example, implies that enterprises need to take a holistic approach to designing and implementing their next-generation security architecture.



Where it all comes together.™

VeriSign leverages deep expertise, proven methodologies, and state-of-the-art tools to help enterprises develop a cost-effective and scalable architecture for network access. VeriSign consultants objectively evaluate an enterprise's existing architecture and then identify and prioritize the gaps in meeting business priorities and user demand.

+ VeriSign® Unified Authentication

VeriSign Unified Authentication allows enterprises to significantly reduce the risk of unauthorized access while dramatically reducing the costs associated with strong authentication. Along with its technology partners, VeriSign enables enterprises to easily deploy and manage a variety of strong authentication solutions, including digital certificates, dynamic one-time passwords, and USB tokens with smart card technology—to minimize, if not eliminate, unauthorized access, while reducing costs.

- **Digital certificates**—The VeriSign® Managed PKI enables enterprises to leverage the VeriSign global PKI infrastructure to seamlessly issue and manage a large number of digital certificates.
- **USB tokens**—VeriSign produces a variety of tokens that provide “smart-card” functionality (in plugged-in mode), one-time-password generation, and secure storage, at a significantly lower cost than other solutions.
- **Dynamic One-Time Passwords**—Unified Authentication supports the authentication of any form of dynamic one-time passwords that are compliant with the Initiative for Open Authentication (OATH).

In addition, VeriSign Managed PKI provides out-of-the-box integration with leading VPNs (such as Cisco Systems®, Check Point®, and Nortel®) to protect data while in transit across public networks by enabling Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) security.

Because VeriSign solutions are based on mature, proven services that integrate easily with existing technology resources, enterprises can rapidly strengthen security while minimizing the costs associated with developing, deploying, and maintaining in-house digital-certificate services.

+ Managed VPN

VeriSign MSS simplify and strengthen perimeter security by allowing enterprises to offload security and infrastructure management to a team of experts whose core business is security. VeriSign manages both firewall-resident VPNs and standalone VPN devices (such as, Cisco Systems® Concentrator). The suite of services, which can be utilized individually or as a set, includes assessment, monitoring, management, incident response, and reporting. Working from the VeriSign constellation of globally linked network operation control centers, security teams use sophisticated tools to monitor, correlate, and analyze data across multiple levels of the organization in order to rapidly identify and prevent attacks. Enterprises maintain full control of security policies and decisions and can access network data 24/7 via a Web-based customer portal.

+ For More Information

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit www.verisign.com/products/pki.

Visit us at www.Verisign.com for more information.