



DATA SHEET



## Securing the Mobile Workforce with VeriSign Unified Authentication

With an increasingly mobile workforce, secure remote access for employees is becoming an essential IT requirement. Remote access is typically provided using traditional IPsec Virtual Private Networks (VPN) or newer SSL VPN appliances. VPNs add an additional layer of complexity to network security, are often unstable, and require installation and maintenance of VPN clients on remote users' computers. Though SSL VPNs do not require installation or maintenance of clients, they still require an additional network layer. Additionally, VPN and SSL VPN solutions rely on single-factor authentication - username and password - for secure logon. Providing an additional two-factor authentication layer can add significant complexity and cost and impede an enterprises' ability to secure existing remote or mobile users, or provide new users with remote access.

Adding VeriSign® Unified Authentication and the VeriSign One-Time Password (OTP) or VeriSign Secure Storage token to a VPN or SSL VPN deployment provides for secure remote access that eases complexity at the network level, and provides an easy to use device for remote users. Best of all, with VeriSign Unified Authentication, total cost of ownership can be reduced by as much as 40 percent.

VeriSign Unified Authentication reduces the complexity and cost of strong authentication by providing a single, highly scalable platform for managing all types of two-factor authentication credentials. The VeriSign One-Time Password Token enables strong authentication through an easy-to-use and highly cost effective token that complies with the OATH standard and comes with a full warranty.



The VeriSign Secure Storage Token is the industry's first all-in one token to combine OTPs and PKI authentication with Secure Storage and Smart Card technology, enabling a variety of security-related applications. The token includes a USB flash drive that connects to a computer's USB port to enable the transfer and encryption of files to and from the storage device. A user PIN is all that is required to quickly and easily access and decrypt files for removal from the device. This personal and versatile mobile device is the perfect solution for unifying authentication and encryption mechanisms to protect employee's credentials and sensitive information.



Where it all comes together.™

### + Leverage Your Existing Technology Investments

Based on open standards, VeriSign Unified Authentication relies on well-established protocols such as Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-in User Service (RADIUS), and Transport Layer Security-Extensible Authentication Protocol (TLS-EAP) to allow easy integration, cross-platform interoperability, and rapid deployment on virtually any device, application, or network. Companies do not have to deploy new software or hardware and can leverage existing enterprise directories and identity management infrastructure. The solution includes easy-to-use application programming interfaces (APIs) for integrating with existing applications, and support for the VeriSign PKI is built in to many leading applications. To simplify token management and provisioning in enterprises, the service integrates an enterprise's existing corporate directory, the directory management console, as well as SSO and AAA solutions for identity management.

### + Flexible Deployment Options

**VeriSign-hosted Validation.** To ensure continuous availability, VeriSign Unified Authentication offers a validation service built on the proven VeriSign Domain Name System (DNS) infrastructure. All critical security components (e.g., OTP vault, Certificate Authority infrastructure, and PKI roots) reside on the DNS network, and all functions (e.g., OTP and digital certificate verification) are executed there. The globally distributed DNS network has a fully redundant infrastructure with 24/7 service support and 99.999 percent uptime, enabling services to leverage the VeriSign infrastructure to deliver superior availability. This option scales smoothly from hundreds to millions of users, ensuring high performance and allowing enterprises to deploy strong authentication on an as-needed basis.

**In-premise Validation Engine.** VeriSign also offers an in-premise validation solution for enterprises. This in-premise validation module is built with the same technology as VeriSign-hosted Validation. Enterprises will be able to utilize the VeriSign highly scalable validation software and the single, integrated management platform, which leverages an enterprise's existing infrastructure while providing uncompromised reliability and scalability.

### + Full Administrative Control

VeriSign Unified Authentication includes a Web-based management console that automates user enrollment and consolidates credential provisioning and lifecycle management. Administrators can issue, revoke, renew, recover, and audit OTP keys and digital certificates from a single, unified interface. Enterprises maintain full control over internal security policies and user information. All user identities, credential templates, and authorization policies remain within the enterprise directory under the strict supervision of the enterprise. VeriSign never views or stores enterprise data.



### Self-Service Applications

The built-in VeriSign Unified Authentication self-services help minimize support costs by enabling users to perform most lifecycle operations on their own. Users can access self-service applications through either of the following user interfaces:

- Web interface. Enables users to access self-service applications through a Web interface to enterprise-hosted token management services.
- Programming interface. To enable the integration of the user self-services into existing user portal or existing customer support applications, VeriSign also provides an integration SDK.

Besides issuing new credentials, OTP token activation, and certificate auto-enrollment, the self-service applications enable users to:

- Synchronize a token
- Replace a lost or broken token
- Enroll for new certificates or renew existing one

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," TeraGuard, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

10-25-2005