VeriSign® Unified Authentication for Windows® Applications

IT departments are increasingly overwhelmed by demands from employees to access corporate information anywhere, anytime to remain competitive in a global business environment. Yet continued growth of malicious attacks on corporate networks demands more stringent security mechanisms and conclusive proof of employee identity before granting access to the corporate network. For Windows® environments, this means making user access more secure for Microsoft® Windows® logon, Outlook® Web Access, Wi-Fi networks, and remote access for Windows desktops.

VeriSign® Unified Authentication is a strong authentication platform consisting of multi-purpose authentication tokens, combined with highly flexible software and services. Together, VeriSign and Microsoft are delivering the added security, inherent to two-factor authentication, to Windows network applications. Strong authentication, which requires users to possess a second, physical factor such as a token or smartcard in addition to a password, is widely recognized as an essential component for protecting against the various forms of security attacks prevalent today.

Unified Authentication provides solutions for a variety of Windows network applications including:

- **Microsoft Windows Logon:** Unified Authentication provides secure Windows desktop logon, whether inside or outside the corporate network, through smartcard Logon and One-Time Password (OTP) – no password caching or smartcard reader is required.
- **Microsoft Outlook Web Access:** Unified Authentication provides an out-of-box solution to enable email access to remote employees through a Web-based interface.
- **Wi-Fi Networks:** Unified Authentication can be used to issue EAP-TLS client certificates to employees to increase Windows Wi-Fi network security and protect against malicious rogue users and devices.
- **Remote Access for Windows Desktop:** Through an additional integration of Unified Authentication and Citrix® Metaframe®, users can access remote corporate resources from home or any external network via their Windows desktop over a Web interface.

Unified Authentication is a single, integrated platform for Windows that can manage multiple user credential types such as digital certificates and OTP tokens. By leveraging key Windows backend components such as Microsoft® IAS server, Microsoft® Active Directory, and Microsoft® Management Console, Windows based enterprises do not have to invest in a different infrastructure to support two-factor authentication for their network access applications.

VeriSign Unified Authentication enables enterprises to utilize a single integrated platform for all their strong authentication needs. Unified Authentication reduces the cost of deployment by leveraging an enterprise's existing infrastructure while moving the complexity of security and scalability to VeriSign. Based on guidelines developed by Initiative for Open Authentication (OATH), the open reference architecture provides a common interface for managing all types of credentials from multiple vendors. By reducing the cost and complexity of strong authentication, the Unified Authentication solution enables more ubiquitous adoption of strong authentication, thereby propelling enterprises to the next level of innovation, sophistication, and complexity in online collaboration and commerce.

At VeriSign, we believe security shouldn't put you on the defensive. Done properly, security should free you to confidently pursue opportunities in commerce, communication, and collaboration. To do this requires significant security expertise to assess, design, deploy, and manage your security plan based on best practices and Intelligence and Control. For more information on how the VeriSign Unified Authentication solution will assist you to achieve your Intelligence and Control goals, please contact our Unified Authentication Specialists at 650-426-5310 or email unifiedauthentication@verisign.com.

VeriSign operates intelligent infrastructure services that enable enterprises and individuals to find, connect, secure, and transact across today's global computer networks.