



DATA SHEET

KEY BENEFITS

Flexible and extensible

By managing multiple credentials on a single platform, VeriSign Unified Authentication enables enterprises to leverage a single integrated platform for all their strong authentication needs. With the flexibility to run validation at VeriSign or within the enterprise, Unified Authentication supports all users—employees, partners, and customers. In the future, enterprises will achieve secure federated networks across suppliers, business partners, and customers.

Multipurpose

Next-Generation Tokens

More than just an authentication device, the easy to use Multipurpose Next-Generation Token can be used in unplugged mode as a clientless OTP token. Using PKI certificates, the Multipurpose Next-Generation Token can be used in connected mode as a USB smartcard device, allowing for the most secure authentication of digital signatures and data encryption. In the future, you will see generations of this device that will have secure mass storage as well as static password management.

VeriSign® Unified Authentication

Enterprises frequently deploy multiple authentication mechanisms to address diverse usage scenarios within and beyond the corporate network. The most common scenarios that need strong authentication are remote access, windows logon, and Wi-Fi access. However, provisioning and managing strong authentication mechanisms like One-Time Passwords (OTPs), USB tokens, and public key infrastructure (PKI) can be a complex and costly task. 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. Built on VeriSign's global trust network, the open, interoperable, and federated platform enables enterprises to strongly authenticate virtually any user, device, or application, on any network. VeriSign Unified Authentication also enables encryption, digital signing, and auditing.

Strong authentication mechanisms can be used on enterprise desktops or externally by using a next-generation hybrid token that allows users to conveniently carry all security credentials with them. Designed for rapid deployment and easy integration, the solution leverages existing enterprise identity management infrastructure while preserving enterprise control over user data, security policies, and certificate lifecycle management. Using the VeriSign Unified Authentication solution to strengthen and streamline security, enterprises gain the freedom and control to respond agilely to new opportunities and changing markets.

+Single Authentication Platform for Multiple Credentials

Unlike multi-vendor or piecemeal point solutions, VeriSign Unified Authentication provides a single platform for provisioning, managing, and using multiple authentication credentials. The platform supports strong authentication using smartcards, device-generated OTPs, and digital certificates. It also supports PKI-based encryption, digital signing, and non-repudiation. Enterprises can quickly and cost-effectively issue OTPs and digital certificates to employees, customers, and business partners, and in the future will be able to manage device certificates.

+ Next-Generation Token

The VeriSign Multipurpose Next-Generation Token is a core component of the VeriSign Unified Authentication solution and allows users to carry OTP and PKI credentials wherever they go. With all credentials stored on this single, portable token, users can conveniently access all the resources for which they are entitled—from virtually anywhere. In unplugged mode, the token can be used to generate OTPs for clientless authentication to applications where the user may not have access to a USB drive



Where it all comes together.™



Integrated and Open

Built on known, open, industry standards like LDAP and RADIUS, VeriSign Unified Authentication leverages an enterprise's existing IT infrastructure. Companies can easily integrate and deploy using their existing central user directory, user provisioning and SSO middleware, AAA servers, and administration tools.

Highest security, reliability, and scale without the complexity

The VeriSign Unified Authentication service architecture enables small to Internet-scale user deployments while moving the complexity of security, reliability, and scale to VeriSign's Internet infrastructure. With a history of issuing more than five million credentials—and a fully redundant globally distributed DNS infrastructure—VeriSign is uniquely positioned to deliver unmatched reliability, scalability, and best-of-breed security.

Lower TCO

With cost-effective tokens, user self-service modules that reduce on-going management and maintenance, and by leveraging existing infrastructures, companies will lower their Total Cost of Ownership by 25 to 40 percent over other two-factor authentication solutions.

(i.e., kiosks, terminals, etc.). To obtain an OTP, the user presses a button on the token, which is coded to dynamically generate passwords that will only work for that particular user. The resulting password appears on the token's LCD. The user enters the OTP into the application's password field, along with his or her user ID and static personal password or PIN. OTP authentication does not require client software and is ideal for allowing partners, customers, and remote employees to access extranets and virtual private networks.

When plugged in (via the USB connector), the token can be utilized as a secure PKI credential store. These PKI credentials can be used to authenticate, digitally sign, and encrypt email, Web-based forms, transactions, and other confidential data. In addition, an embedded smartcard chip on the token allows storage of other identifying information regarding the user or enterprise.

+ 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

In-the-cloud Validation Utility. To ensure continuous availability, VeriSign Unified Authentication offers a validation service built on VeriSign's proven 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 the



In-the-cloud Validation Utility. Enterprises will be able to utilize VeriSign's 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 helps 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

+ Industry Compliance

The PKI component of VeriSign Unified Authentication is available in a version that complies with the Federal Bridge Certification Authority (FBCA), allowing enterprises to interoperate easily with federal agency PKIs. In addition, the PKI helps enterprises comply with industry-specific government mandates regarding the protection, availability, and audit-ability of sensitive data. Using Unified Authentication's PKI functionality, healthcare services providers, financial institutions, government agencies, insurance companies, and other organizations can authenticate, encrypt, sign, and audit data exchanges to support compliance with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill 1386, the Gramm-Leach-Bliley Act, and 21 CFR Part 11.

+ Learn More

For more information about VeriSign Unified Authentication, please call 650-426-5310 or email unifiedauthentication@verisign.com.

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