



## DATA SHEET

### KEY BENEFITS

#### *More value*

Unified Authentication delivers more value with next-generation OTP, hybrid and storage tokens on a single integrated platform.

#### *Less cost*

Enterprises gain up to 60% lower TCO with cost-effective tokens without adding new infrastructure and by deploying user self-service applications. Unified Authentication leverages investments in existing infrastructures, including the central user directory, user provision and SSO middleware, AAA servers and administration tools, enabling an easily integrated and deployed solution.

#### *Designed to fit*

Provides maximum deployment flexibility with the option of using an in-the-cloud validation utility or an in-premise validation engine for those enterprises that require more control of the overall infrastructure.

#### *Future proof*

VeriSign Unified Authentication offers an open solution as opposed to a proprietary one and gives you continuous innovation to grow with your business.

## 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 the VeriSign 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 any one of the VeriSign tokens. 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 smart cards, 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.

### **+ VeriSign Tokens**

At the core of the VeriSign Unified Authentication solution is the VeriSign One-Time Password (OTP) Token, the VeriSign Secure Storage Token and the VeriSign USB Token.



Where it all comes together.™



### VeriSign One-Time Password Token



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 for the duration of your service (3 to 5 year plans available).

### VeriSign Multipurpose Next-Generation Token



The VeriSign Multipurpose Next-Generation Token is the industry's first all-in-one security token. A single token can generate dynamic OTPs and store digital certificates (for PKI-based authentication, encryption, digital signing and non-repudiation), and smart card information. Using the token's OTP authentication capabilities, partners, customers and mobile employees can strongly authenticate themselves from virtually any location or device, whether or not the access point has a USB port.

### VeriSign Secure Storage Token



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 employees' credentials and sensitive information.

### VeriSign USB Token



The VeriSign USB token can store multiple user PKI credentials for strong authentication and other security-related tasks. It can be used at any workstation or device that has a USB port, providing greater portability and convenience. The USB token can also be used as a smart card login device for SSO functionality.



### + 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% 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 utilise 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 enrolment 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 authorisation policies remain within the enterprise directory under the strict supervision of the enterprise. VeriSign never views or stores enterprise data.



## DATA SHEET

### *VeriSign Australia*

For more information, please call us at +61 3 9674 5555, or email [enterprise-sales@verisign.com.au](mailto:enterprise-sales@verisign.com.au)

### *VeriSign Hong Kong*

For more information, please call us at +852 2153 8161, or email [HKsales@verisign.com](mailto:HKsales@verisign.com)

### *VeriSign Singapore*

For more information, please call +65 9023 5301, or email [enterprise-sales@verisign.com.sg](mailto:enterprise-sales@verisign.com.sg)

### Self-Service Applications

The built-in VeriSign Unified Authentication self-services help minimise 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-enrolment, the self-service applications enable users to:

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

### + Industry Compliance

PKI helps enterprises comply with industry-specific government mandates regarding the protection, availability and audit-ability of sensitive data. Using the Unified Authentication Authentication PKI functionality, healthcare services providers, financial institutions, government agencies, insurance companies and other organisations can authenticate, authenticate, encrypt, sign and audit data exchanges to support compliance with federal regulations such as the National Privacy Principles, under the Privacy Act, introduced on 21 December 2001.

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