



## DATA SHEET

### KEY BENEFITS

#### *Provides a single, unified platform for strongly authenticating all users and all devices across all networks*

An open, interoperable, federated platform and a hybrid USB token unify provisioning, management and use of multiple authentication credentials.

#### *Authenticates Users Regardless of Location*

The VeriSign Unified Authentication Service stores onetime passwords (OTPs), smart-card chips and digital certificates on a single USB token, enabling partners, customers and employees to use authentication credentials from any location.

#### *Enables Rapid, Widespread Deployment of Authentication Credentials*

By making the most of the enterprise's existing directory infrastructure and VeriSign's highly scalable managed service, enterprises can easily issue and manage authentication credentials for thousands of end users and network devices.

## VeriSign® Unified Authentication Service

Enterprises frequently deploy multiple authentication mechanisms to address diverse usage scenarios within and beyond the corporate network. However, provisioning and managing public key infrastructure (PKI), onetime passwords (OTPs) and USB tokens can be a complex and costly task. The VeriSign® Unified Authentication Service 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 authenticate virtually any user, device, or application reliably, on any network. The service 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 carry all security credentials conveniently with them. Designed for rapid deployment and easy integration, the service employs existing enterprise identity management infrastructure while preserving enterprise control over user data, security policies and certificate lifecycle management. Using the VeriSign Unified Authentication Service to strengthen and streamline security, enterprises gain the freedom and control to respond with agility to new opportunities and changing markets.

### + Single Authentication Platform for Multiple Credentials

Unlike multi-vendor or piecemeal point solutions, the VeriSign Unified Authentication Service 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 not only to employees, customers and business partners but also to Web services applications and network devices such as servers, routers and firewalls.

### + Next-Generation Token

VeriSign's hybrid USB token is a core component of the VeriSign Unified Authentication Service and allows users to carry PKI, OTP and smart-card credentials wherever they go. With all credentials stored on this single, portable



Where it all comes together.™

### *Minimises Deployment and Administration Costs*

Consolidated credential provisioning and management reduce cost of ownership when compared with multi-vendor and piecemeal point solutions.

### *Supports Compliance with Government Mandates*

Enterprises can make the most of OTPs and digital certificate services such as authentication, encryption, digital signing and non-repudiation to promote compliance with industry-specific regulations regarding data privacy.

### *Promotes Identity Federation and Adoption by Partners, Customers and Suppliers*

VeriSign's proven platform is recognised and trusted throughout the world, encouraging rapid adoption of authentication services both within and outside the enterprise.

### *Reduces Risk Exposure*

By delegating key security tasks and processes to a proven industry leader, enterprises minimise the risks and penalties associated with improper deployment or operation of an internal authentication solution.

token, users can conveniently access all the resources to which they are entitled - from virtually anywhere. In unplugged mode, the token can be used to generate OTPs at terminals, kiosks and other devices that lack a USB port.

To obtain an OTP, the user presses a button on the token, which is coded to generate passwords dynamically for only that particular user. The resulting password appears on the token's liquid crystal display (LCD). The user enters the OTP into the application's password field, along with his or her user ID and static personal password. 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) and endowed with PKI capabilities, the token can be used to authenticate, digitally sign and encrypt email, Web-based forms, transactions and other confidential data. In addition, an embedded smart-card chip on the token allows storage of other identifying information regarding the user or enterprise.

### **+ Standards-Based Integration**

Based on open standards, the VeriSign Unified Authentication Service relies on well-established protocols such as the Lightweight Directory Access Protocol (LDAP), the Remote Authentication Dial-in User Service (RADIUS) and the 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. Enterprises do not have to deploy new software or hardware and can employ existing enterprise directories and identity-management infrastructure. The service includes easy-to-use application programming interfaces (APIs) for integrating with existing applications and support for the VeriSign PKI is built into many leading applications. To simplify token management and provisioning in enterprises using Microsoft® servers and desktops, the service tightly integrates with Microsoft client software and Microsoft® Active Directory Server®, Microsoft® Internet Information Services, the Microsoft® Internet Authentication Service, and the Microsoft® Management Console®. To simplify access control, the VeriSign Unified Authentication Service also integrates tightly with IBM® Tivoli Access Manager™ and applications that use it.

### **+ Full Administrative Control**

The VeriSign Unified Authentication Service 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 and 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.

### **+ Proven Infrastructure**

To ensure continuous availability, the VeriSign Unified Authentication Service is built on VeriSign's proven domain name system (DNS) infrastructure. All critical security components (such as the OTP vault, the certificate authority infrastructure, and the PKI roots) reside on the DNS network, and all functions



(such as OTP and digital certificate verification) are executed there. The globally distributed DNS network has a fully redundant infrastructure with service support 24 hours a day, 7 days a week and 99.999 percent uptime, enabling services that use that infrastructure to deliver superior availability. In addition, the service scales smoothly from hundreds to millions of users, ensuring high performance and allowing enterprises to deploy authentication services as needed.

#### **+ Industry Compliance**

The PKI component of the VeriSign Unified Authentication Service 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 protection, availability and auditability of sensitive data. Using the service's PKI functionality, providers of health-care services, financial institutions, government agencies, insurance companies and other organisations can authenticate, encrypt, sign and audit data exchanges to support compliance with governmental legislation.

#### **+ For More Information**

For more information about VeriSign Unified Authentication Service, please call 0800 032 2101 or email [sales@verisign.co.uk](mailto:sales@verisign.co.uk).

**Visit [www.verisign.co.uk](http://www.verisign.co.uk) for more information.**