



DATA SHEET



KEY FEATURES

Unified interface for smart card and digital certificate management

A single easy-to-use Web-based interface allows organizations to securely enroll card holders and manage the entire lifecycle of cards and digital certificates.

Multiple issuing models

Various deployment models are supported: bureau for large volume deployments, batch for groups of users, individual for face-to-face service, and self-service.

Numerous roles and card policies

Access to the system is controlled through definable roles and an unlimited number of card policies

Supports contact and contactless cards

Manage proprietary cryptographic cards, Java cards, iClass, and MIFARE interfaces.

Range of Technology Vendors

Support for multiple vendors of smart cards and middleware, USB devices, biometric solutions, card printers, LDAP directories, and HR systems.

Full audit trail and flexible reporting

All system activity is logged into a security audit database. Multiple reports can be defined, produced, viewed and printed using the integrated reporting tool.

VeriSign® Unified Authentication – Smart Cards

Enterprises and government agencies frequently deploy multiple authentication mechanisms to address diverse requirements within and beyond their networks and facilities. More and more they are using smart card-based credentials as they aim to increase security, address regulatory compliance pressures, and lower costs through the use of merged physical and logical access credentials. VeriSign® Unified Authentication is a single, integrated platform for the provisioning and management of all types of strong authentication credentials, including digital certificates, one-time password (OTP) tokens, and smart cards.

VeriSign® Unified Authentication – Smart Cards is a comprehensive and easy-to-use suite of management tools specifically designed for smart card deployments, supporting a wide choice of smart card types, workflows, and deployment options for securing enterprises and government agencies. It includes a fully featured card management system, addressing the entire smart card credential life cycle, from card and credential issuance to replacement and cancellation, as well as managing smart badging and applets. Together with VeriSign® Unified Authentication - PKI, VeriSign® Unified Authentication – Smart Cards provides a highly integrated credential management solution.

+ Easy-to-Use and Quick-to-Deploy

VeriSign® Unified Authentication – Smart Cards is extremely easy to use. Users are automatically guided, step-by-step, through issuance and management tasks using unique and patented secure workflow technology. The self-service Web portal feature enables end users to perform smart card and credential management functions without requiring the help of an administrator. Users can unlock smart cards, request temporary credentials, and handle digital certificate renewals. The self-service portal enables users to quickly address their credentialing needs, which allows them to promptly resume their work.

Since the PKI and smart card components of the solution are pre-integrated out-of-the-box, the whole system can be deployed in days, saving the time and money usually spent on complex custom integration and troubleshooting.



Where it all comes together.™



KEY FEATURES

Consolidation and Completeness

VeriSign® Unified Authentication – Smart Cards, with VeriSign® Unified Authentication – PKI, allows for a wide choice of authentication mechanisms including digital certificates, USB tokens, and smart cards which can all be managed with a single system. If required, it can also be extended to operate in conjunction with VeriSign® Unified Authentication – OTP.

Ease of Deployment

VeriSign® Unified Authentication – Smart Cards and PKI is an out-of-the-box solution which allows for seamless integration or will layer over an existing PKI smoothly.

Ease of Use

Credential administrators have only one system for issuing, revoking, and managing all users' credentials for both physical and logical access.

Simplified User Experience

End users also only have one system to use if any of their credentials are lost or need renewal.

Cost Effectiveness

A common infrastructure for physical and logical systems derives economy of scale.

+ Interoperability and Scalability

Since a card management system will be integrated into a number of third party infrastructure components, such as smart card middleware, PKI services, physical access control software, and authentication devices, it is necessary for it to be highly interoperable. VeriSign® Unified Authentication – Smart Cards supports a variety of third party technologies, providing a highly-scalable, future proof system which can grow with the organization's ever expanding needs.

Through standardization on a single multi-purpose credential storage container, smart cards and USB tokens can lead to cost savings, increased ease-of-use for users and improved security. The ability to reduce—via a multi-purpose smart card or USB token—the number of credentials issued makes it easier for organizations to utilize multi-factor authentication for stronger security. Users no longer need to be concerned with multiple credentials, or remember which credential belongs to which application. Furthermore, connecting the process for granting and revoking physical and logical access helps organizations adhere to regulations that require assurances of strong authentication and access control. Auditing capabilities allow organizations to enforce and manage these requirements.

+ Enhanced Flexibility with Tight Policy Control

VeriSign® Unified Authentication – Smart Cards gives organizations the freedom to choose the most appropriate device and credential issuing models for their needs. Bulk importing of card holder details, an easy-to-use self service portal, and a personalization bureau interface ensure that enterprises have full flexibility. Access to the system can be controlled through definable roles, with an unlimited number of policies for issuing and managing credentials. This guarantees organizations the flexibility they need to meet their security objectives.

+ Meeting Regulatory Requirements

Homeland Security Presidential Directive 12 (HSPD 12) mandates that all US Federal Government employees and contractors are to be issued standardized smart cards and digital certificates, as specified by the FIPS 201 and Personal Identity Verification (PIV) standards.

By connecting the process for registration, identity-proofing, issuance and maintenance of PIV cards for physical and logical access, VeriSign® Unified Authentication – Smart Cards aids US Federal Government Agencies and other organizations to quickly comply with the processes defined in FIPS 201. Furthermore, since all system activity is logged into a security audit database with extensive reporting capabilities, organizations can easily enforce and manage rigid regulatory requirements. VeriSign® Unified Authentication – Smart Cards is a pre-packaged and integrated PIV and Shared Service Provider (SSP) solution.

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

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," 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.