



## Extending Managed PKI Services to Smart Cards

for Greater Convenience and Security



## CONTENTS

Executive Summary	1
The Convenience and Security Continuum	1
PASSWORDS	2
PERSONAL IDENTIFICATION NUMBERS (PINs)	2
DIGITAL CERTIFICATES	2
SMART CARDS	2
SMART CARDS AND DIGITAL CERTIFICATES	2
SMART CARD PRIVACY	2
VeriSign Managed PKI	3
VeriSign Certificate Issuance Solutions for Smart Card Providers	3
VERISIGN HIGH-VOLUME CERTIFICATE ISSUANCE SOLUTION	4
VERISIGN MEDIUM-AND LOW-VOLUME CERTIFICATE ISSUANCE SOLUTION	5
Passport to Convenience and Security	6
FINANCIAL SERVICES	6
GOVERNMENT	6
COLLEGES AND UNIVERSITIES	7
WIRELESS APPLICATIONS AND SERVICES	7
From Here...	7

**Executive Summary**

The Internet offers unprecedented opportunities for enterprises to provide 24-hour convenience, increase revenues, reduce costs, and keep ahead of competitors. Government agencies, too, can harness the ubiquity and convenience of the Internet to reduce costs and improve the efficiency of delivering services to citizens and businesses. To fully realise these benefits, enterprises, governments, and other entities require an affordable solution that enables them to efficiently and securely exchange strategic information anywhere, anytime, while providing customer convenience and personalisation.

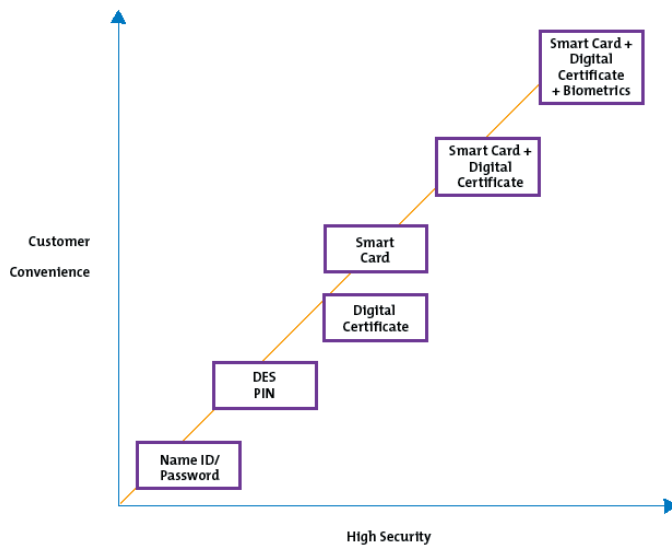
In choosing security technologies, the selection process becomes one of weighing risks and costs. Although passwords and PIN authentication are the most widely used security methods, they are also the least secure. The strongest form of authentication available today comes via hardware devices, such as smart cards combined with digital certificates. Used within a public key infrastructure, smart cards provide an efficient, secure, flexible, and portable medium for authenticating identities, encrypting data, and auditing transactions. The financial, education, healthcare, and wireless industries, as well as governments throughout the world, are early adopters of Public Key Infrastructure (PKI)-enabled smart card solutions, leveraging their security features and portability to alleviate security risks, reduce costs, and provide customers with convenient, sophisticated services.

As the leader in Internet trust services, VeriSign extends its managed digital certificate services to enable smart card and other device manufacturers to embed digital keys and certificates into their products. VeriSign’s scalable certificate issuance solutions for smart cards accommodate a range of certificate issuance needs and enable faster time to market for all sizes of consumer and business applications by allowing organizations to flexibly issue millions of certificates per year or only a few.

**The Convenience and Security Continuum**

Early computer security solutions started with user IDs and passwords and then evolved to include PINs, digital certificates, and smart cards. As technology becomes more advanced, security solutions provide not only stronger security, but also greater customer convenience. The most secure, convenient, and practical solution today comes from combining PKI technology—digital certificates—into smart cards.

Figure 1 – Security Solutions



**PASSWORDS**

Although passwords are commonly used in relatively low-risk environments, they are inconvenient and inadequate for the high-value transactions and communications that travel across the Internet. Passwords are easy to break, and users often write down or share passwords, or forget them. In addition, different applications require new IDs and passwords. Moreover, passwords by themselves cannot provide often-required security services: They do not ensure privacy (through encryption); they cannot guarantee the integrity of stored or transmitted data (through digital signing); and they cannot legally prove that a party participated in a transaction (non-repudiation).

**PERSONAL IDENTIFICATION NUMBERS (PINs)**

Because the user must provide an access token and a personal identification number (PIN), security is stronger than with a password alone. However, a PIN (on its own) cannot provide important security services such as privacy, data integrity, and non-repudiation.

**DIGITAL CERTIFICATES**

Digital certificates are the preferred technology over passwords and PINs for securing electronic transactions of all types. Based on public key encryption, digital certificates serve as unique, unforgeable online credentials, authenticating the identity of each device or device user and identifying privileges and attributes for authorised access to private online information. In addition to being a superior mechanism for identity authentication, digital certificates provide the privacy, data integrity, and non-repudiation services that are not supported by passwords and PINs. In most applications, digital certificates reside on the user's hard drive.

**SMART CARDS**

Smart cards carry an embedded microchip that stores data and applications. Smart cards hold more information than magnetic stripe cards and can be programmed for a variety of applications. Multiple applications can reside on a single smart card, and applications can be added, deleted, or upgraded without reissuing the card.

**SMART CARDS WITH DIGITAL CERTIFICATES**

Smart cards that use digital certificates offer greater security, convenience, and portability for Internet-based business than other security solutions. Placing the digital certificate and key pair on the smart card provides more protection against theft or impersonation than if they were stored on the user's hard drive, and requiring a PIN to access the user's credentials on the smart card provides an added layer of protection if the smart card itself is lost or stolen. Networks, systems, and applications are much less likely to be compromised. In addition, by incorporating one or more identification certificates on the smart card, users can carry with them the appropriate credentials to access systems remotely, forever severing ties to a single workstation.

**SMART CARD PRIVACY**

In addition to the security issues addressed by smart cards and PKI, the use of a smart card strengthens the ability of systems to protect individual privacy and guard against identity theft.

### VeriSign Managed PKI

Digital certificates are based on Public Key Infrastructure—the architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. This system uses a pair of mathematically-related keys to encrypt and decrypt confidential information and to generate and verify digital signatures. A public key infrastructure reduces the risks of fraud and other unauthorised access by enabling enterprises to authenticate employees, partners, customers, and other users; encrypt communications and transactions; offer secure online payment capabilities; and audit transactions.

Extending the VeriSign managed PKI solution to incorporate digital certificates onto smart cards increases the level of authentication for users and provides mobility and confidence for conducting sensitive transactions from personal computers, wireless devices, and remote computer terminals. VeriSign managed PKI is a fully integrated service designed to secure intranet, extranet, email, virtual private network, and e-commerce applications. It enables enterprises to cost-effectively establish a robust, customised PKI and Certification Authority (CA) system for issuing, renewing, and revoking digital certificates, without having to build their own internal security infrastructure.

Unlike software-only solutions or building a PKI in-house, the VeriSign managed PKI service lets organisations control certificate registration and policies, while VeriSign provides the back-bone of certificate processing. By leveraging the VeriSign certificate processing infrastructure, enterprises can implement a PKI solution in a matter of days, and can take advantage of VeriSign's proven capability to offer trusted, scalable managed services.

In Australia, VeriSign's Managed PKI services are managed through the Regional Operations Centre (ROC) in Melbourne, Victoria. This world-class facility is security accredited to 'Highly Protected' by the Australian Security Intelligence Organisation (ASIO) as part of the Commonwealth Government's Gatekeeper scheme. VeriSign's infrastructure is designed, evaluated, and audited by the leading authorities in the field, including ASIO, Defence Signals Directorate, Defence Science & Technology Organisation (DSTO), and Ernst & Young. The infrastructure is backed by binding Service Level Agreements, a disaster recovery infrastructure, high-security facilities, screened personnel, and customer support.

### VeriSign Certificate Issuance Solutions for Smart Card Providers

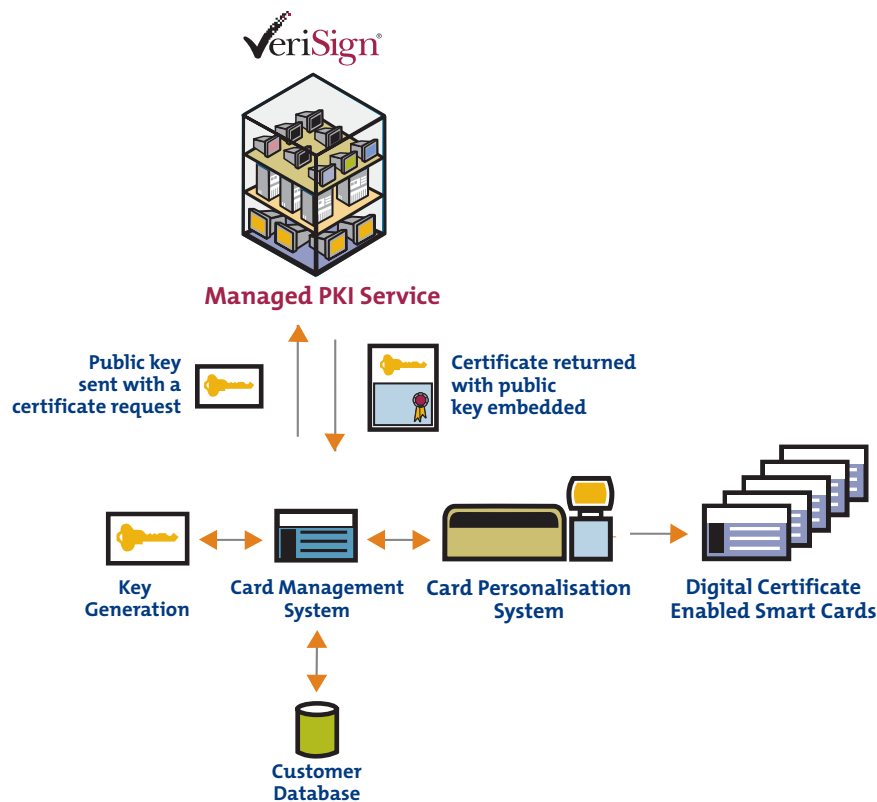
VeriSign, the leading provider of Internet trust services, offers scalable, flexible, and customisable solutions for embedding certificates into smart cards. The VeriSign solutions for small-, medium-, and large-volume certificate issuance are device agnostic, and support multiple processes including key generation and certificate issuance. By allowing enterprises to outsource all or a portion of the certificate issuance process, VeriSign solutions make it easier and faster to produce and integrate certificates onto smart cards for a range of purposes—from mobile phones to banking, healthcare, and national ID cards. The range of offerings allows enterprises to choose an appropriate level of control in the process of key generation and certificate issuance. In addition, enterprises can leverage the expertise of VeriSign's Professional Services Organisation to provide seamless integration with existing systems and services.

**VERISIGN HIGH-VOLUME CERTIFICATE ISSUANCE SOLUTION**

VeriSign provides a platform that enables certificates to be generated in batch volumes for incorporation into smart cards and other devices. The platform, based on VeriSign’s carrier-class, 24x7 digital certificate architecture and industry-leading outsourced managed services, is currently the only offering that enables smart card providers to scalably integrate digital certificates into the device manufacturing/card production process. VeriSign can integrate with various device manufacturing systems or card management systems via the XML key management specification (XKMS) standard interface or through direct integration.

By using the VeriSign platform, enterprises can centrally generate digital certificates in volumes based on their scheduled production quantities. The VeriSign platform provides scalability and reliability with little effort or resources expended by the enterprise. Keys are virtually impossible to break and because they are generated before the cards are branded and printed, this helps the issuer catch potential problems with key or certificate generation before the cards are embossed and personalised.

Figure 2 – High-Volume Roll Out of Digital Enabled Smart Cards



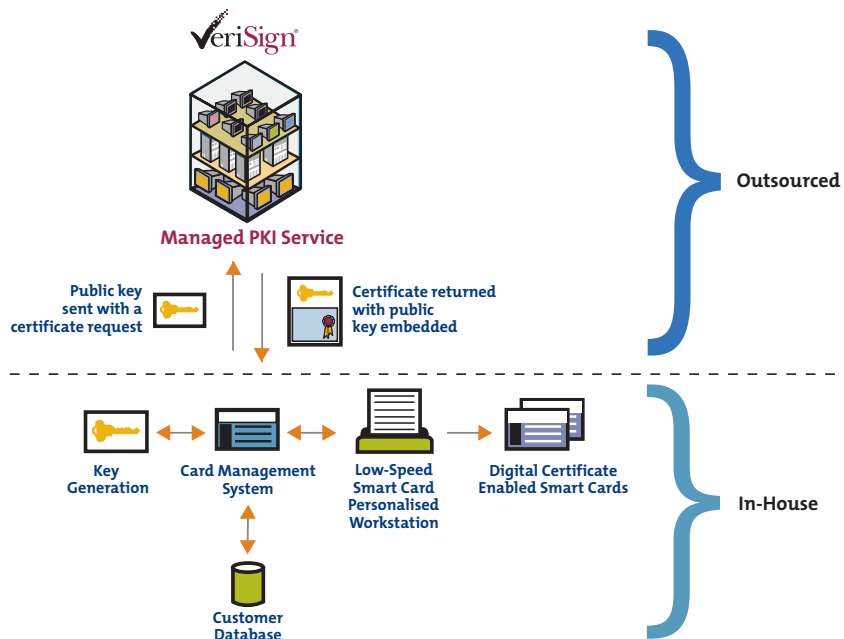
**VERISIGN MEDIUM-AND LOW-VOLUME CERTIFICATE ISSUANCE SOLUTION**

Medium-and low-volume certificate issuance solutions are ideal for enterprises or situations that require limited numbers of certificates to be flexibly issued at any given time including for the introduction of pilot programs, the issuance of security badges, or the handling of exceptions such as lost cards.

For example, a bank may want to distribute smart cards to a specific number of customers for financial and banking applications. In this scenario, the bank utilises a smart card vendor's card management system (CMS) located at the bank to manage the customer data. The CMS sends a certificate request along with the public key to VeriSign for the generation of a certificate. VeriSign generates the certificate and sends it back to the CMS. The CMS combines additional user data, keys, and the certificate into a file which is forwarded to a personalisation system where the smart cards are produced and distributed.

The certificate enrolment process can also be initiated directly by the end user, in which case the enrollment information and key generation occurs at the user's workstation and smart card reader. This information (along with the public key) is then approved by a central administrator within the user's organisation, sent to VeriSign for certificate issuance, and the certificate is then issued to the end-user and incorporated onto the smart card. The CMS also facilitates post issuance services for the smart card, whereby a user may update information or add new information to their card via a standard web interface operated by the central administrator or organisation.

Figure 3 – Low-to-Medium Volume Roll-Out of Digital Certificate Enabled Smart Cards



## Passport to Convenience and Security

When used with PKI services, smart cards strengthen security and unlock the door to tremendous levels of convenience. The inherent portability of smart cards allows them to go wherever users go, allowing enterprises to expand their customer base, offer new services electronically, and manage security more confidently and efficiently. Financial institutions, government agencies, colleges and universities, and wireless services are rapidly adopting smart cards with digital certificates to provide their customers with a convenient, multi-purpose passport to a wide range of applications and services.

### FINANCIAL SERVICES

Customers expect easy access to a broad range of services from their financial institutions, and they demand high standards of security, convenience, and value. Credit cards and debit cards offer convenience but they also are subject to fraud. In addition, financial institutions now have to compete with telecommunications, software, and other industries that include smart card technology in their products. Smart cards with a PKI solution help financial institutions retain existing customers as well as attract new customers. For example, banks can offer consumer smart cards that not only incorporate credit, cash, and debit services within the same card; but also enable customers to make Web-based purchases, carry multiple currencies on a single card, and pay for transportation. Using smart cards, banks can dynamically adjust credit lines to reflect the unique risk profile of each customer.

The opportunities among corporate customers are equally compelling. To engage in high-value, business-to-business e-commerce requires the capability to electronically verify identities among financial institutions and businesses, as well as to protect sensitive data. In addition, enterprises must be able to eliminate the risk of transaction repudiation. When used with an integrated Identrus solution (see sidebar), smart cards allow banks and other financial institutions to leverage their traditional role as trusted third parties to offer their corporate customers a secure, convenient framework for electronically verifying the identity of their trading partners around the world. Corporate customers can shorten the negotiation and transaction lifecycles using smart cards with VeriSign digital certificates to check credit and identity; encrypt sensitive data; and digitally sign business documents, payments, and agreements.

### GOVERNMENT

When used with a PKI, smart cards enable governments to safely provide citizens, employees, suppliers, and partners quick access to critical programs and information while reducing operating costs and improving customer satisfaction. Citizens can obtain smart cards that allow them to access confidential information, obtain benefits electronically, and pay for government services. For example, using a single card, a citizen might look up his or her military records, receive a medical insurance benefit, or pay a road toll. Employees can use cards for procurement, travel expenses, or accessing classified data.

To provide better service and reduce costs, several agencies of the United States government- including the General Services Administration (GSA), Department of Defense, and the Veterans Health Administration-are beginning to implement ambitious smart card programs.

The US Government uses smart cards for multiple purposes, including easy portability of military and civilian medical data, military personnel records, and financial entitlements data including purchasing authority and phone calling card services. More recently the government has explored using smart cards to store private keys and digital certificates, often with other data to create multi-purpose cards.

**COLLEGES AND UNIVERSITIES**

Today's educational institutions are under increasing pressure to reduce costs while providing a quality academic experience for students. PKI-enabled smart cards allow schools to not only reduce administrative costs, but also provide greater convenience to students—without sacrificing service or education. Students can use their digitally-secured smart card to gain access to restricted buildings and lab equipment, register for classes, receive test scores, and check out books from the library. They can also use it as a multi-purpose payment card, charging books, debiting the price of tickets from their bank accounts, or paying with pre-paid vouchers for vending machine products.

**WIRELESS APPLICATIONS AND SERVICES**

Wireless applications are changing the face of the Internet. Users can use digital phones, personal digital assistants, and pagers to transfer money, access medical records, make travel reservations, and more. But before engaging in wireless transactions, users must be confident that they can reliably identify and authenticate each other, as well as protect information from interception or tampering. When used with VeriSign digital certificates, the smart card's portability makes it the ideal mechanism for ensuring security in wireless applications.

**From Here...**

Although digital certificate-embedded smart cards are rapidly becoming the medium of choice for providing a single point of secure access to broad applications, their adoption is still in its infancy. Like the Internet itself, smart card applications and technologies will become more sophisticated as issuers and users begin to understand and expand the ways in which smart card technology can be applied to secure transaction exchange.

The key to remaining ahead of the curve in this exciting new world is a PKI infrastructure that provides the scalability, stability, and interoperability to grow with an organisation as it adds new applications and services. As the leader in managed PKI services and as an innovator in smart card solutions, VeriSign provides products with proven scalability, reliability, and interoperability for enterprises poised to take the next step in the digital revolution.

**For More Information**

For additional VeriSign product and pricing information, please call us at +61 3 9674 5555, send us an email at [enterprise-sales@verisign.com.au](mailto:enterprise-sales@verisign.com.au) or visit the VeriSign Australia Web site at: <http://www.verisign.com.au/>

**About VeriSign Australia**

VeriSign Australia was established in July 1999 to provide Internet trust services to Australian companies, websites and individuals. Its suite of services includes domain name, authentication, payment, wireless and validation services, enabling it to serve as a gateway for any business wishing to establish or grow its online identity and Web presence.

**About VeriSign**

VeriSign, Inc. (Nasdaq:VRSN) is the worldwide leader in providing digital trust services that enable businesses and consumers to use digital networks with confidence. Digital trust services create a trusted environment through three core offerings — Web identity, authentication and payment services — powered by an infrastructure that manages more than five billion communications and transactions a day.

©2004 VeriSign, Inc. All rights reserved.  
VeriSign, the VeriSign logo, The Value of Trust, Payflow, Payflow Link, Payflow Pro, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. VSA0408