WHITE PAPER:
NATIONAL PKI: THE FOUNDATION OF TRUST IN GOVERNMENT

The Foundation of Trust in Government Programs

National PKI

Who should read this paper

Governments around the world are gearing up to deliver the next generation of services to their citizens. To provide such services, governments need robust and scalable technologies and policies to execute trusted transactions and establish trusted identities. Strong credentials based on public key infrastructure (PKI) are the answer. By employing the right mix of authentication, encryption, and digital signatures, governments can significantly reduce the risk of forgery, theft, or abuse of identification credentials. This in turn allows them to secure their borders, protect and allocate public assets and resources, meet their fiduciary responsibilities, and boost overall citizen satisfaction.

Confidence in a connected world. Symantec.

National PKI

The Foundation of Trust in Government Programs

Contents

Introduction 1

Why governments urgently need PKI 1

PKI: The path to a more secure state 2

Facilitate the growth of e-government 2

Implement effective national ID programs 3

Administer secure e-passport programs 3

What to look for in a PKI provider 4

The Symantec PKI solution 5

Why choose Symantec? 7

Conclusion: Now is the time for PKI 7

Glossary. 8

Introduction

Governments around the world are gearing up to deliver the next generation of services to their citizens. They want to accept digitally signed tax returns. Execute electronic transactions securely. Tighten border control. They want to do all of this while maintaining strong security, streamlining administration, and containing operational costs. The challenge is significant. To provide such services, governments need robust and scalable technologies and policies to execute trusted transactions and establish trusted identities. And these technologies must be capable of being leveraged for identity-sensitive services provided by businesses and other non-governmental organizations, such as e-commerce and online banking.

Many governments have taken first steps toward implementing security technologies and policies. They have created digitally enhanced travel and identity documents, issued smart healthcare and tax ID cards, and implemented business authentication services. But governments have an obligation to move beyond implementing merely adequate protection mechanisms to deploying the gold standard of safeguards against transaction fraud, identity theft, duplication, and/or spoofing.

Strong credentials based on public key infrastructure (PKI) are the answer. By employing the right mix of authentication, encryption, and digital signatures, governments can significantly reduce the risk of forgery, theft, or abuse of identification credentials. This in turn allows them to secure their borders, protect and allocate public assets and resources, meet their fiduciary responsibilities, and boost overall citizen satisfaction.

Additionally, the trust that PKI engenders leads directly to significant cost savings. Because PKI enables them to securely authenticate a person, organization, or device, governments can streamline processes and complete transactions in a fraction of the time and for a fraction of the cost of what it would take using other, less advanced, security mechanisms. PKI also opens up opportunities for joint efforts by governments and businesses to make citizens' lives more convenient, productive, and secure.

To seize these opportunities while minimizing the risks that accompany complex technology deployments, governments need the right PKI partner. Symantec is that partner. As the leading enabler of trust on the Internet, Symantec delivers a proven PKI platform that enables governments to deploy Internet-age authentication processes today while maintaining flexibility of their investments for tomorrow. And because the Symantec platform leverages the same industry-leading PKI service that has made Symantec a global leader in managed PKI solutions — a service that has already been deployed for hundreds of millions of users in large-scale self-contained PKI projects around the world — government authorities and public bodies know they are backed by an industry leader.

This white paper starts with a PKI primer that introduces the technology. It then outlines the three most common government applications of the technology. Finally, it shows how the Symantec PKI solution can be used to provide robust protection against the fraudulent reproduction and misuse of government IDs to engender a more productive, fiscally responsible, and secure society.

Why governments urgently need PKI

Traditional identification credentials are neither robust enough to protect against modern fraud, nor can they enable the next generation of applications, such as digitally signed tax returns, electronic tenders, and seamless border control. Instead, governments require the strong authentication, encryption, and digital signatures that are part of a comprehensive and scalable PKI platform.

PKI is the foundation on which governments can execute secure and trusted transactions. Whether between individuals and governments; businesses and governments; or inter-government relationships, PKI allows public entities to securely authenticate all participants in a

transaction. A combination of hardware, software, facilities, people, policies, and processes, PKI can be leveraged to create, manage, store, distribute, and revoke the digital certificates that lie at the heart of a trusted identity system.

PKI is designed to ensure the security and trustworthiness of transactions and identities in three ways: through authentication, encryption, and digital signatures.

- **Authentication.** Authentication is achieved by binding public and private keys to user identities through a certificate authority (CA). Each user identity issued by a CA is unique, so that a credential issued that is based on PKI can be trusted.
- **Encryption.** Another way that PKI promotes trust is through encryption. The CA simultaneously creates public and private keys for an individual. The private key is kept private by that individual and never shared with anyone or sent over the Internet. The public key is stored in a directory as part of a digital certificate. Anyone who wants to send a secure message uses the public key of the recipient to encrypt it. The recipient is the only one who can decrypt it, using his or her private key.
- **Digital signatures.** By far the biggest impact that PKI is expected to have in both public and private sectors is its ability to create and validate digital signatures to ensure the non-repudiation of transactions. A digital signature is created with an algorithm that combines an individual's private key with the electronic document that is being signed. Since only the person who owns the private key can create the digital signature, that signature can be trusted. This can be verified by anyone possessing the public key for that individual.

PKI: The path to a more secure state

PKI has emerged as the trusted technology of choice for ensuring the trustworthiness of identity credentials in three key areas: e-government, national identity programs, and e-passport programs.

Facilitate the growth of e-government

E-government is the cornerstone of the next-generation of government. Citizens, businesses, and government agencies are already benefiting from their ability to access services and conduct transactions online. E-government programs allow government organizations to deliver services, distribute resources, and administer programs more efficiently, which drives operational costs down.

PKI plays a critical role in e-government by allowing governments to leverage authentication, encryption, and digital signature technologies when issuing identity certificates, business certificates, and device certificates.

The trust enabled by these certificates helps governments:

- **Streamline operations.** Day-to-day activities such as procurement, tax processing, and benefits administration can be executed online, thus more efficiently.
- **Minimize the risk of fraud and waste.** This allows governments to protect public assets and conserve funds at a time when tax revenues are dropping precipitously around the globe.
- **Disseminate information more easily and securely.** By giving citizens convenient online access to such private information as tax and land records, as well as other sensitive data that previously existed only in paper form, governments can increase citizen satisfaction even as they reduce costs.
- **Partner with industry.** Whether issuing an identity credential in the form of a smart card, token, or other kind of soft certificate, governments must ensure that this credential can be leveraged in non-government applications. This is easily achieved by choosing the right partner and by building interoperability and scalability into the PKI program design.

Implement effective national ID programs

As part of a global trend toward issuing more secure identity documents, an increasingly large number of countries have started issuing national ID cards. These smart cards can be used to access healthcare services, verify employment, and complete online transactions. Countries such as Belgium, Spain, and Germany have already implemented highly successful national identification programs. Indeed, global shipment of smart cards were estimated to grow around 10% in 2010 and reached 6 billion.[1]

PKI provides a common framework for issuing verifiable identities through a natural trust hierarchy. These identities can then be used to electronically sign and encrypt documents for transactions such as filing taxes, redeeming benefits, or applying for jobs. By implementing national ID programs using PKI, governments can improve the security of the data stored on an ID card and promote greater use of the card in non-government applications such as e-commerce, banking, and social networking.

National ID programs with PKI enable governments to:

- **More effectively allocate public resources.** As the costs associated with healthcare, pensions, and other public entitlements escalate, it has become critical to distribute these resources fairly and efficiently.
- **Secure virtual and physical facilities.** Implementing access control so that only authorized persons gain access to sensitive information and secure areas has never been more important.
- **Secure non-government relationships.** PKI credentials can be used to authenticate users who wish to access commercial online services or sign e-commerce transactions digitally. This makes PKI an invaluable element of any successful ID program.
- **Meet international compliance standards for data security and privacy.** Standards such as those established by the Euro Banking Association and International Standards Organization (ISO), as well as the myriad individual privacy acts passed by individual countries, mandate strong authentication and data integrity.
- **Participate in interoperability programs.** Several projects have been launched by the European Union to promote standards and collaboration for interoperability in e-procurement, identity, and electronic signatures. PKI is the foundation for trust in all of these programs, including Secure IdenTity AcrOss BoRders LinKed (STORK), Pan-European Public Procurement Online (PEPPOL), and European Patient Smart Open Services (epSOS).

Administer secure e-passport programs

An e-passport is a combination paper and electronic document with an embedded chip that holds digital signature-confirmed data. A broad range of governments and industries, including the European Union (EU), Gulf Country Communities (GCC), and International Civil Aviation Authority (ICAO), have collaborated to establish global standards that ensure travelers can quickly be authenticated as they move from country to country. E-passports are already being used by a growing list of countries, including the United States, Belgium, Austria, Australia, Norway, Spain, and the United Kingdom.

PKI is essential to e-passport programs, as it is used to create the digital certificates used by governments to digitally sign an e-passport at the time it is issued. Additionally, PKI is the foundation for the ICAO Public Key Directory (PKD), which facilitates a trust hierarchy that is leveraged to verify the authenticity of travel documents.

1-"Smart Card Market Forecast to 2012," RNCOS, January 2011

PKI-based e-passport programs allow governments to:

- **Streamline border crossings and customs processes.** Moving from one country to another is fraught with paperwork and delays. E-passports make these transitions easier and less painful for citizens through standards created by ICAO.
- **Reduce the risk of forgery and fraud.** Traditional paper passports are notoriously easy to forge and/or steal and repackage. The digital signatures capability of PKI can mitigate such risks.
- **Maintain detailed information on citizens' movements in and out of the country.** Because this information can be sensitive, and subject to strict privacy laws, strong security mechanisms are needed to protect the rights of individual citizens.
- **Work with other governments on cross-border law enforcement initiatives.** Particularly after 9/11, governments have been attempting to collaborate more closely on anti-terrorist, anti-drug, and other law enforcement activities. E-passports can enable more effective tracking of individuals traveling from one country to another.

What to look for in a PKI provider

The benefits of PKI are substantial. But implementing traditional PKI solutions is notoriously difficult due to the large number of components involved and the degree of integration required. The difference between success and failure lies in partner selection. The right PKI platform from the right partner enables governments to:

- **Comply with standards.** Many international standards are very specific about the ways that PKI-based systems must implement certificate profiles and modify policies. They also require a deep understanding of complex hierarchies. As standards for PKI interoperability continue to evolve, it is important that a government's PKI partner supports technological advancements in a way that enables them to comply with these mandates.
- **Protect their investments in PKI.** If implemented correctly, a PKI platform is not just the foundation for building robust e-passports, national ID, or e-government programs. It also gives governments the ability to continue enhancing and expanding citizen services in the future. Rather than having to re-architect a completely new platform for new initiatives, a successful PKI deployment will set the stage for future successes.
- **Scale the platform as their needs grow.**Many national identification programs begin small, with pilot tests or for limited use such as drivers' license or healthcare programs. A PKI vendor must deliver a solution that enables governments to expand these programs without worrying about outgrowing their capacity or capabilities.
- **Integrate all identity programs onto a single PKI platform.** A successful PKI deployment establishes a single platform that can be used for all identity-related programs, including, but not limited to, national ID, e-passports, and e-government. This requires the use of open standards that make these programs interoperable with each other and with legacy systems.
- **Tap into a broad ecosystem of supporting technology vendors and integrators.** No one vendor can do it all. Open standards are a cornerstone of interoperability. In addition, your PKI partner should have strong relationships with other technology providers and integrators that can enable seamless deployment of the plethora of technologies and services required to successfully implement a PKI platform.
- **Support non-government organizations' PKI efforts.** A strong PKI partner for government programs will be able to co-develop services for commercial partners across a broad range of industries.
- **Minimize the costs of PKI deployment.** PKI is a complex technology. It takes highly experienced professionals dedicated to PKI deployments to implement successfully. Without such experience, implementations can take much longer than anticipated, resulting in significant cost overruns.

- **Implement policy, training, and knowledge transfer programs.** The policies and trusted personnel that support PKI are as important as the technology. A PKI partner should have a strong background in developing PKI policies, an in-depth PKI training program, and an understanding of the importance of knowledge transfer.

The Symantec PKI solution

As a robust on-premise PKI solution, the VeriSign® Certificate Lifecycle Platform from Symantec provides the same rich functionality and robust architecture that Symantec employs for the thousands of customers that use its other managed PKI services. And it does this while giving governments control, since all components — CAs as well as data — can be kept within their borders. Figure 1 shows the architecture of Certificate Lifecycle Platform.

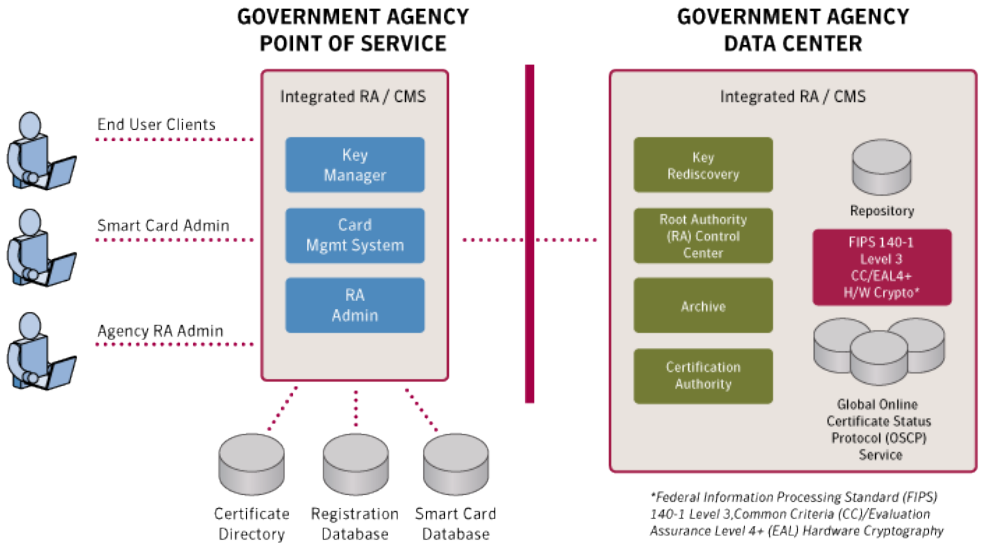

Figure 1: Symantec PKI Solution

In addition, Certificate Lifecycle Platform:

- **Is highly scalable and extensible.**Developed to operate on a multiprocessor distributed architecture, Certificate Lifecycle Platform contains high-performance transaction engines and scalable database systems, including the Sun Microsystems Solaris™ operating system and Oracle® database on the back end, and UNIX® and Microsoft Windows® on the front end. Additionally, components of Certificate Lifecycle Platform can be distributed across multiple servers to support very high workloads and availability requirements. Designed to scale from thousands to hundreds of millions of user credentials, it is extensible in a way that allows governments to take advantage of new services and solutions as they become available from service providers.
- **Enables tight integration with leading card management systems.** Symantec supports easy, rapid deployment of PKI applications and strong authentication using smart cards across major Web browsers and platforms. This helps governments that wish to simplify high-volume delivery of PKI digital certificates and applications via the latest generation of smart cards.
- **Offers flexible certificate validation service.** Certificate Lifecycle Platform uses the online certificate status protocol (OCSP) that allows applications and users to determine a certificate status in real time. As an alternative to certificate revocation lists (CRLs), OCSP may be used to obtain additional status information on demand, and offers the option of providing hourly updates to its CRLs rather than the standard 24-hour refresh. Symantec's validation service is trusted by and can scale to millions of businesses, government organizations, and end users on a daily basis.

- **Provides full certificate lifecycle management capabilities.** Certificate Lifecycle Platform is designed for large in-premise configurations where a managed PKI solution is not appropriate. Certificate Lifecycle Platform gives governments end-to-end control over their PKI infrastructure, and is capable of supporting millions of end user digital certificates on a global scale. Figure 2 shows Certificate Lifecycle Platform architecture in detail.

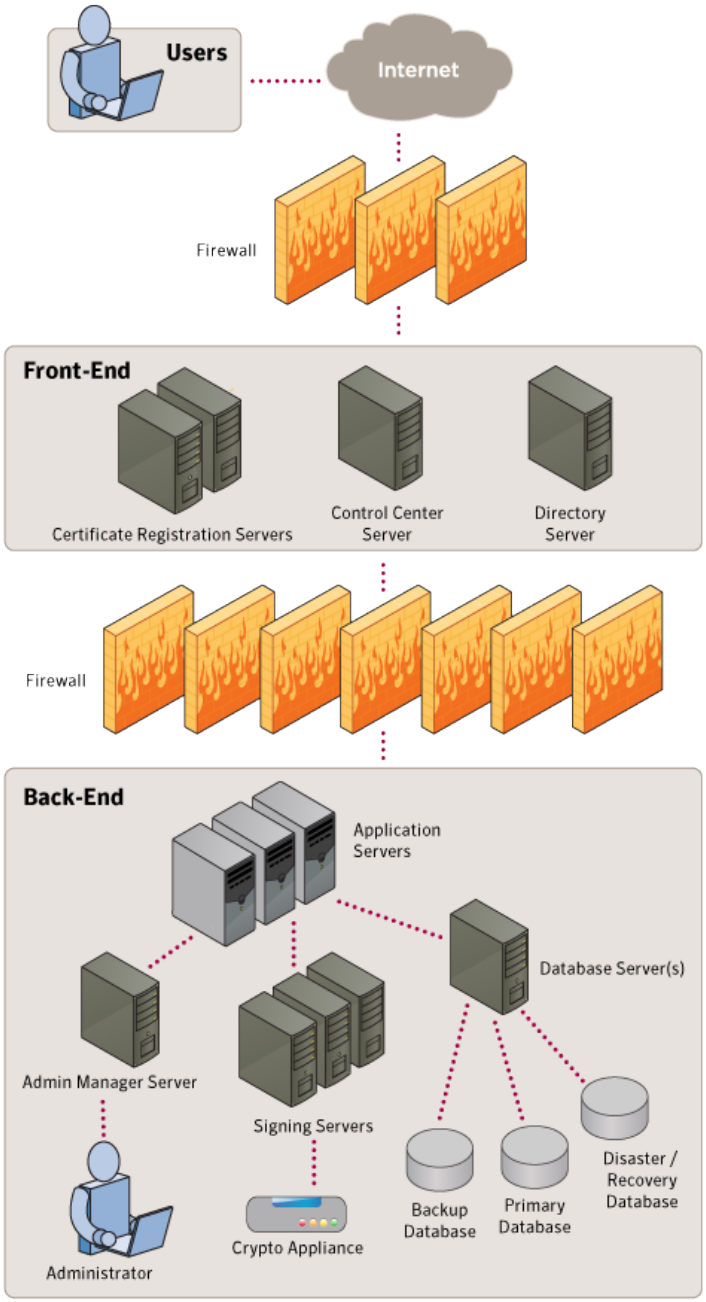

Figure 2: VeriSign Certificate Lifecycle Platform Architecture

- **Supports open standards.** Symantec leverages a highly available infrastructure that supports open standards and protocols including X.509, Lightweight Directory Access Protocol (LDAP), Open Database Connectivity (ODBC), Remote Authentication Dial-In User Service (RADIUS), and Open AuTHentication (OATH).

Why choose Symantec?

Symantec has the longest running cloud-based PKI platform on the market, with more than twelve years of experience and hundreds of millions of digital certificates issued worldwide. Additionally, Symantec has:

- **A trusted reputation.** Symantec is the SSL certificate provider of choice for more than 93 percent of the Fortune 500 and 97 of the 100 largest banks in the world. Consumers, businesses, and governments alike trust Symantec for online security and identity protection because of its robust infrastructure and rigorous business authentication practices.
- **The ability to scale and evolve as new technologies become available.** Every year, products are entering the market with more sophisticated native PKI support. As a result, digital certificates may be installed on a growing range of open standards-based devices including computers, tokens, smart cards, mobile devices, and more. Certificate Lifecycle Platform and its standards-based approach offer governments the flexibility they need to evolve their PKI implementations as the technology continues to evolve.
- **Global reach.** Symantec's PKI platform has been selected by numerous leading government organizations that require end-to-end control of a high-grade PKI solution to secure sensitive information. Applications include: military, government ID programs, and intelligence operations.
- **Industry expertise.** Symantec is a premier provider of PKI services to the financial services, e-commerce, manufacturing, and healthcare markets worldwide. Symantec can leverage this experience and expertise not only to drive value for governments themselves, but to enable them to develop services that can be leveraged by industry partners.
- **Experience with large-scale deployments.** Symantec currently runs more than 20 large-scale PKI data centers worldwide, including British Telecom, DSV, KPN/Getronics, Adacom, Shikoku/Tohoku Electric, NTT DoCoMo, ADP, Macau Post, and CertiSign.

Conclusion: Now is the time for PKI

PKI implementations have reached critical mass. Today, all SSL servers use PKI; all Web browsers support PKI; in a number of countries, citizens can file tax returns using PKI certificates; countless commercial banks use PKI for online banking; and the scientific community requires PKI. Today, thousands of organizations — in both the public and private sectors — depend upon PKI to ensure that identity-sensitive services are delivered in a safe and secure manner.

Most significantly, partnerships between government PKI-based programs and commercial entities mean that PKI investments can be leveraged across both public and commercial applications. With interoperability between national ID cards, commercial smart cards, e-passports, e-commerce transactions and other forms of identity-sensitive services, governments, industry, and individuals can all benefit equally from the world's accelerating adoption of PKI.

Glossary

Certificate Authority (CA)	An entity that leverages PKI to issues digital certificates for use by other parties. The CA is authorized to issue, suspend, or revoke certificates.
Certificate Revocation List (CRL)	A periodically issued list, digitally signed by a CA, of identified certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked certificates' serial numbers, and the specific times and reasons for revocation.
Certification Practices Statement (CPS)	A document containing a statement that specifies the practices a CA or RA employs in issuing certificates. This document is revised as necessary by the CA.
Credential	The artifact produced after an individual or entity has been sufficiently authenticated. Credentials come in the form of digital certificates, tokens, smart cards, mobile phones, or installed software, and may be used to enable strong or multi-factor authentication.
Digital Certificate	An electronic document that uses a digital signature to bind a public key to an identity belonging to an entity. The entity can be an individual, a device, or an organization. The certificate can then be used to verify that the public key indeed belongs to that entity.
Digital Signature	The digital equivalent of a handwritten signature. Digital signatures are cryptographically-based and provide non-repudiation, which means they can be legally used as evidence that the sender of a given message sent it, and that a recipient indeed received it.
Key Generation	The trustworthy process for generating, documenting, and storing public keys and private keys.
Online Certificate Status Protocol (OCSP)	A protocol for providing parties with real-time certificate status information.

Operational Period	The period that starts with the date and time a certificate is issued or activated and ends with the date and time it expires or is revoked.
Premium CRL	A CRL that is updated more frequently than a standard CRL and made available to customers who have purchased premium CRL access.
Private Key	The mathematical key (kept secret by the holder) used to create digital signatures and decrypt messages or files encrypted with the corresponding public key.
Public Key	The publicly available mathematical key that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key.
Public Key Infrastructure (PKI)	An umbrella term used to describe all the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke a digital certificate.
Registration Authority (RA)	An entity approved by a CA to assist persons in applying and/or revoking or suspending certificates. The RA also approves applications for certificates. An RA is not the agent of a certificate applicant, and may not delegate the authority to approve certificate applications to anyone other than authorized RAAs.
Registration Authority Administrator (RAA)	An employee of an RA who is responsible for carrying out the functions of an RA.
Smart Card	A credit card-sized card with an embedded processor and memory that can receive input, process it, and provide output. Smart cards are typically used to provide strong authentication of identity for businesses and government organizations.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign, VeriSign Trust and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. Other names may be trademarks of their respective owners.

7/2011 21195844