INSTALLATION GUIDE

Managed PKI v7.2

Introduction

VeriSign, Inc. ■ March 2008

DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign, Inc. has made efforts to ensure the accuracy and completeness of the information in this document. However, VeriSign, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein.VeriSign, Inc. assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, VeriSign, Inc. assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner. VeriSign Inc. reserves the right to make changes to any information herein without further notice.

TRADEMARKS

VeriSign, the VeriSign logo, “Where it all comes together.”, Intelligence and Control, VeriSign Trust Network, Unified Authentication, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Other trademarks and service marks in this document are the property of their respective owners.

This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this VeriSign product. If you need help using this product, contact customer support.

enterprise-pkisupport@verisign.com

+1-650-426-3535 or 1-800-579-2848

Publication date: March 2008

Contents

Introduction

VeriSign Managed PKI is a public key infrastructure (PKI) platform. As a PKI system, Managed PKI protects the confidentiality and integrity of electronic communications. This guide provides an overview of the Managed PKI product. Designed to orient new users, *Managed PKI Introduction* explains the primary concepts and services involved in Managed PKI.

This chapter includes the following topics:

About Public Key Infrastructure (PKI)

PKI, or public-key infrastructure, is the combination of software, encryption technologies, and services that enables your company to protect the security of your Internet communications and business transactions. PKI uses digital certificates called Digital IDs, public-key cryptography, and Certification Authorities (CA) to create an enterprise-wide network security architecture that protects against intrusion, such as hackers who steal passwords or intercept email messages and credit card transactions.

Digital IDs, also known as certificates*,* authenticate parties and secure communications in electronic communications. Certificates are electronic documents that identify individuals, organizations, computer servers, and computer devices, such as wireless devices. As with a driver's license or passport, a certificate provides proof of identity. For example, certificates may be used to prove one's identity in order to access sensitive intranet and Internet information, thereby replacing expensive and cumbersome user names and passwords.

PKI provides the following benefits:

- **Authentication**. Assurance that the sender of a message is, in fact, who they say they are. For a signed email message, authentication checks that the digital signature on the signed message is valid. Authentication may also be used to confirm the identity of a Web site.

- **Privacy**. Assurance that no one but the recipient can view an encrypted message.
- **Authorization**. Ability to provide or restrict access to sensitive information or Web resources.
- **Integrity of Data**. Verification that a message has not been altered by another party in transit.
- **Nonrepudiation**. Provides evidence of the origin or delivery of data. Nonrepudiation makes it impossible for the sender of a signed message to claim that he or she did not send the message, or that he or she sent a different message.

VeriSign Managed PKI

Implementing a PKI solution can be a complex and costly process, requiring highly-skilled personnel and complex hardware and software systems. VeriSign Managed PKI provides an integrated PKI platform for you, combining enterprise controlled and operated PKI software and hardware, compatibility with popular applications, and the certificate processing services and infrastructure of the VeriSign back end.

To implement your own PKI solution, you would need to set up systems, telecommunications, databases, physical site security, Internet-safe network configurations, high-availability redundant systems, disaster recovery, PKI specialists, viable PKI legal practices, and financially safe PKI liability. Managed PKI provides this infrastructure for you, operating on VeriSign's highly-available and highly-secure PKI back end, thus enabling your organization to reap the benefits of PKI without the risk, effort, and expense of buying and maintaining your own PKI system.

Managed PKI protects the confidentiality and integrity of electronic communications. With Managed PKI, people may encrypt messages to one another, confirm one another's identities, and determine whether messages have been tampered with in transit by unauthorized parties. Managed PKI supports your enterprise around the globe, enabling your users to enroll for Digital IDs and view Digital ID contents in major Asian and European languages.

Your Users and Managed PKI

Users are responsible for enrolling for their Digital ID, renewing the Digital ID when it expires, protecting their private key, and if necessary, revoking their Digital ID. Users may save their Digital ID into their browser, where it may be used for email and accessing intranet and Internet information.

Depending on how your organization implements Managed PKI, your users may use Digital IDs to do the following:

- Access secure online data or services. Users present their Digital ID as proof of their identity.
- Send and receive secure email messages. Managed PKI seamlessly integrates with popular email applications, enabling users to send encrypted email messages and to receive and decrypt encrypted email messages from other users.

Administration and Management of Managed PKI

Your organization must appoint individuals to administer and maintain Managed PKI. Managed PKI administrators ensure that Digital IDs are issued only to properly authenticated individuals, in accordance with the practices of your organization and of the VeriSign Certificate Practices Statement (CPS). Administrators review certificate requests and approve or reject them. Administrators download certificate revocation lists (CRLs), lists of certificates that have been revoked, to ensure that invalid certificates are not accepted by the system. Administrators also generate reports, monitor the operation of Managed PKI, and instruct users on the usage of their Digital IDs.

Chapter 2, "About Managed PKI," provides more detailed information on the operation of Managed PKI.

About this Manual

This manual is intended for Managed PKI administrators and other personnel who want to:

- Learn about the options and features available with Managed PKI
- Learn about digital certificates
- Learn about the VeriSign Managed PKI document set
- Prepare to install Managed PKI

Managed PKI Configurations

Managed PKI offers a variety of options and features. Accordingly, you may customize your Managed PKI configuration to meet the needs and requirements of your organization. This manual provides helpful information to assist you in determining which services and features would most benefit your organization. For further assistance in planning your Managed PKI configuration, consult your Account Manager.

Contents of this Manual

This manual is organized as follows:

+ Chapter 2, “About Managed PKI,” discusses the operation and benefits of Managed PKI. Chapter 2 also defines the most commonly used Managed PKI options and services.
+ Chapter 4, “About Certificates,” explains how digital certificates work. Chapter 3 also defines the various types of certificates used with Managed PKI.
+ Chapter 3, “Enrolling For Managed PKI,” reviews the information that a customer needs in order to enroll for Managed PKI. Chapter 4 also explains how to apply for the Managed PKI service and a Managed PKI administrator certificate.
+ Chapter 5, “Managed PKI Directory Structure,” reviews the directory structures that are added to your system when Managed PKI is installed.

VeriSign Managed PKI Documentation

Every customer receives the basic Managed PKI documentation set (see “Managed PKI Basic Documents”). VeriSign also provides additional documentation for customers who buy supplementary packages. Customer documentation is available in PDF format on the Managed PKI Documentation CD and through the Managed PKI Control Center Web site. Since VeriSign wants its documentation to be as useful as possible, we welcome and encourage your input. If you have any comments, suggestions, or questions about this or any other customer document, please contact VeriSign support.

Managed PKI Basic Documents

For all implementations of Managed PKI, VeriSign provides customers with the following documents:

+ *Managed PKI Quick Reference*—A quick reference card to help customers configure Managed PKI.
+ *Managed PKI v7.2 Hardware/Software Requirements*—Lists the requirements needed for Managed PKI and its various features and options.
+ *Managed PKI v7.2 Introduction* (this document)—Provides an overview of Managed PKI products, features, and digital certificates.
+ *Managed PKI v7.2 Getting Started*—Provides information on implementing Managed PKI within your organization and rolling out Digital IDs to your end users.
+ *Enterprise Support and Service Overview*—Describes the support options available with Managed PKI; also, provides contact information for Managed PKI Customer Support.
+ *Managed PKI v7.2 Administrator’s Handbook*—Provides information to assist Managed PKI administrators in managing the Managed PKI certificate subscription service.

- *Managed PKI Installation and Configuration*—Provides the requirements and instructions for the implementation of base Managed PKI, including Local Hosting, VeriSign Registration Authority, and Passcode Authentication, and for moving from pilot Managed PKI to production Managed PKI.
- *Managed PKI 7.2 Technical Reference*—Presents information about the maintenance and functioning of base Managed PKI, such as Local Hosting, Automated Administration, and Passcode Authentication.
- *Managed PKI v7.2 Upgrading*—Contains information to assist customers in upgrading from a previous release of Managed PKI and its associated options and services such as Automated Administration, Key Management Service, and Go Secure! for Microsoft Exchange.
- *Managed PKI v7.2 Glossary*—Defines terms used in VeriSign documentation.
- *Managed PKI v7.2 Error Codes and Troubleshooting Guide* (electronic format only)—Provides descriptions of Managed PKI error codes, along with troubleshooting information.
- *Managed PKI v7.2 Shared Service Provider Configuration Guide*—Provides requirements and instructions for implementing the Shared Service Provider (SSP) option of Managed PKI.
- *Managed PKI v7.2 Certificate Validation Module*—Contains information about Certificate Validation Module (CVM), Certificate Parsing Module (CPM), and Online Certificate Status Protocol (OCSP).

What Should You Read First?

To equip yourself with a basic understanding of Managed PKI, read this document first. For further introductory information, read:

- *Managed PKI Quick Reference*
- *Enterprise Support and Service Overview*
- *Managed PKI v7.2 Administrator's Handbook*
- *Managed PKI v7.2 Getting Started*

VeriSign Managed PKI Web Addresses

Enrollment page: **https://onsite.verisign.com/**
From this page, you can enroll for Managed PKI services, purchase and renew administrator Digital IDs, and renew Managed PKI services.

Control Center: **https://onsite-admin.verisign.com/OnSiteHome.htm**
Using the Control Center, you can view and manage your Managed PKI service.

About Managed PKI

Managed PKI is a PKI platform designed to protect the integrity and confidentiality of electronic communications. PKI systems enable users to confirm one another's identities, encrypt messages to one another, and determine whether messages have been tampered with in transit. This chapter introduces the basic function and components of Managed PKI.

This chapter includes the following topics:

Overview

Designated personnel in your organization, known as Managed PKI administrators (or Local Registration Authorities), control the operation of your Managed PKI system. A person applying for a certificate is known as an applicant. However, once a certificate is downloaded by an applicant, the applicant becomes a subscriber (or end-user subscriber).

For more information about Managed PKI administrators and subscribers, see "Roles and Responsibilities" on page 8.

Certificate Components

Each certificate includes a validity period, a serial number, and the name of the issuing Certification Authority. The validity period is the period of time for which a certificate is valid. To enhance security, all certificates have a limited validity period. A Certification Authority is an entity authorized to issue, suspend, renew, or revoke certificates. When a Certification Authority issues a certificate, the subscriber may securely engage in electronic communications and commerce within your organization's intranet, as well as over the Internet.

For more information about certificates, see Chapter 4, "About Certificates."

Public and Private Keys

For each certificate, a public key and private key are associated with the identity of the certificate holder. Keys are mathematical codes used by communicating parties to encrypt and decipher encoded messages. Encrypting data prevents unauthorized parties from intercepting and accessing sensitive information.

Typically, the sender of a message uses the public key of the recipient to encrypt the contents of the message. The encrypted message can then only be decrypted by the private key of the recipient—no other key will decrypt the message. Upon receipt, the recipient uses his or her private key to decrypt the message.

Public keys are published and widely available, while private keys must be kept secret. For subscribers, public keys and private keys are created when they enroll for certificates. In contrast, Managed PKI administrators receive their public key and private key when they download their Managed PKI administrator ID.

Digital Signatures

Applications that integrate Managed PKI use digital signatures to alert message recipients if an unauthorized party has tampered with the message in transit. A digital signature is a one-way hash attached to a message. A one-way hash is a number of fixed length; it provides a unique identifier for the data contained in the message. If the data in a message is changed by an unauthorized party en route, the value of the hash also changes. If the message has been tampered with, this changed value triggers an alert to the recipient. Unlike the process involved in data encryption, the hash is encrypted and decrypted by the private/public key pair of the sender, rather than the recipient.

Roles and Responsibilities

This section describes the respective roles and responsibilities of subscribers, Managed PKI administrators, and VeriSign's Issuing Center for a basic Managed

PKI implementation. Figure 2-1 shows what the different components of Managed PKI do.

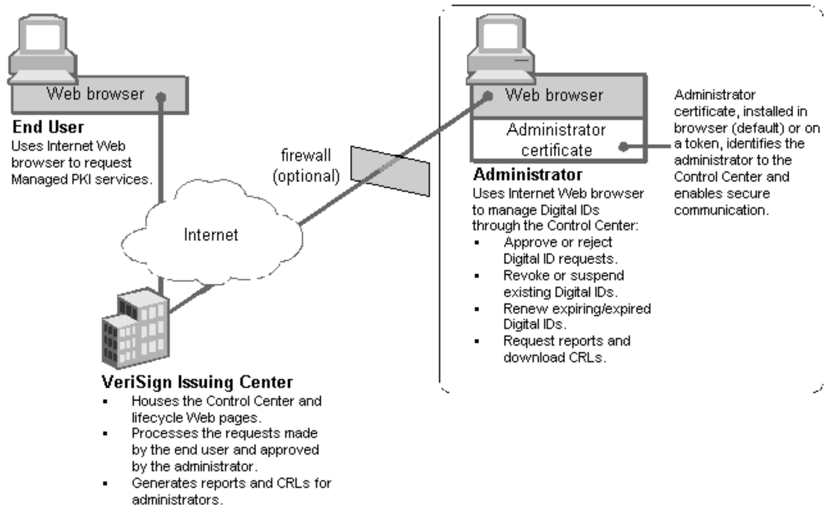
Web browser
End User
Uses Internet Web browser to request Managed PKI services.
firewall (optional)
Internet
Web browser
Administrator certificate
Administrator
Uses Internet Web browser to manage Digital IDs through the Control Center:
▪ Approve or reject Digital ID requests.
▪ Revoke or suspend existing Digital IDs.
▪ Renew expiring/expired Digital IDs.
▪ Request reports and download CRLs.
Administrator certificate, installed in browser (default) or on a token, identifies the administrator to the Control Center and enables secure communication.
VeriSign Issuing Center
▪ Houses the Control Center and lifecycle Web pages.
▪ Processes the requests made by the end user and approved by the administrator.
▪ Generates reports and CRLs for administrators.

Figure 2-1 Basic Managed PKI installation

Subscribers

Using an Internet browser, subscribers are able to perform the following Managed PKI functions:

- Enroll for a new certificate
- Track the status of their application for a certificate
- Retrieve their certificate when it is issued
- Search for and verify another subscriber's certificate
- Renew their existing certificate
- Revoke their own certificate

Requests for new certificates and renewals are sent to the Managed PKI Control Center at VeriSign's Issuing Center for approval. However, subscribers do not require approval for certificate tracking, retrieval, searches, and revocations. Instead, Managed PKI automatically completes these operations, while producing a record of such transactions for the Managed PKI administrator.

Managed PKI Administrator

A Managed PKI administrator (also called Local Registration Authority Administrator, or LRAA) is authorized to review the requests for new IDs and renewals. The Managed PKI administrator may then determine whether to approve or reject the requests.

In addition to reviewing and approving/rejecting certificate requests, the Managed PKI administrator may generate reports, search for account information, and download certificate revocation lists (CRLs). A certificate revocation list includes the certificates that have been suspended or revoked prior to their expiration dates. To perform all of these tasks, the Managed PKI administrator uses the Internet Web browser installed on their computer to access the Managed PKI Control Center, which is hosted at VeriSign's Issuing Center. For information about the Managed PKI Control Center, see *Managed PKI Administrator's Handbook*.

Managed PKI Administrator IDs

The Managed PKI administrator identifies himself or herself to the Managed PKI Control Center with a Managed PKI administrator ID. Managed PKI administrator IDs ensure secure communications by encrypting data sent to VeriSign's Issuing Center. A Managed PKI administrator ID can be installed in the Managed PKI administrator's browser, or on a USB token (a portable data storage device that uses an embedded chip to protect and store certificates). Although Managed PKI installs the certificate in the browser by default, the USB token option provides greater security. Tokens not only protect the certificate with a password, but can also be locked in a secure storage area when not in use. For information on installing a USB token, see *Managed PKI Installation and Configuration*.

VeriSign Issuing Center

The VeriSign Issuing Center is responsible for processing requests for new certificates or renewals. Once the request is approved by the Managed PKI Administrator, the VeriSign Issuing Center issues the certificate. Then, the Issuing Center sends the applicant an email notification of the result. The email notification includes a URL from which the applicant may retrieve the certificate. The Issuing Center also generates reports and certificate revocation lists (CRLs), which are used by Managed PKI administrators to manage Managed PKI customer accounts.

How VeriSign Managed PKI Distributes Certificates

This section outlines the process for requesting, approving, and distributing certificates with a basic Managed PKI implementation (see Figure 2-2 below).

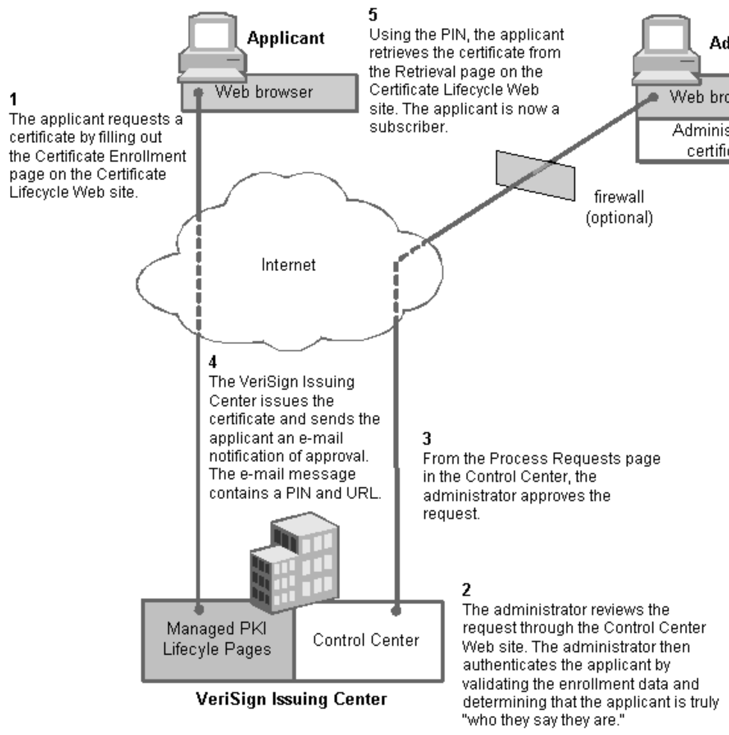
Applicant
Web browser
5
Using the PIN, the applicant retrieves the certificate from the Retrieval page on the Certificate Lifecycle Web site. The applicant is now a subscriber.
Administrator
Web browser
Administrator certificate
1
The applicant requests a certificate by filling out the Certificate Enrollment page on the Certificate Lifecycle Web site.
firewall (optional)
Internet
4
The VeriSign Issuing Center issues the certificate and sends the applicant an e-mail notification of approval. The e-mail message contains a PIN and URL.
3
From the Process Requests page in the Control Center, the administrator approves the request.
2
The administrator reviews the request through the Control Center Web site. The administrator then authenticates the applicant by validating the enrollment data and determining that the applicant is truly "who they say they are."
Managed PKI Lifecyle Pages
Control Center
VeriSign Issuing Center

Figure 2-2 How VeriSign Managed PKI distributes certificates

1 An applicant completes and submits the Web-based Certificate Enrollment form. If the Managed PKI administrator has enabled UTF-8 support, the applicant can enter certificate information in the applicant's native language. Upon completion of the Certificate Enrollment form, the applicant's browser or smart card automatically generates and stores the private and public keys. Then, the Certificate Enrollment form, including the applicant's public key and identification information, is securely transferred to VeriSign. Upon receipt of the form, Managed PKI logs the request for the Managed PKI administrator.

2 Using the Managed PKI administrator ID, the Managed PKI administrator reviews the contents of the enrollment form through the Managed PKI Control Center Web site. Following a well-defined process (described in the organization's *Statement of Practices*), the Managed PKI administrator authenticates the identity of the applicant.

3 After confirming the information in the enrollment form, the Managed PKI administrator approves the request. Once the certificate request is approved, the Managed PKI Control Center automatically sends a message to the VeriSign Issuing Center. Digitally signed by the Managed PKI administrator's private key, the message prompts the Issuing Center to issue a certificate to the applicant.

4 The VeriSign Issuing Center creates and signs the certificate, and sends the new subscriber an email message notifying him or her of the approval. The email message includes a PIN and the URL where the subscriber can retrieve the certificate. Alternatively, the Managed PKI administrator can require the end user to retrieve the certificate in person, adding another precaution for authentication.

5 The new subscriber retrieves the certificate. If the certificate is a public certificate, it may be published in the VeriSign Certificate Repository. To activate this option, the Managed PKI administrator must make the appropriate selection in the *Certificate Publishing Policy* page of the Policy Wizard.

Implementing Managed PKI

Managed PKI offers a wide selection of services, configurations, and optional features. When implementing Managed PKI, your organization must determine which Managed PKI services and features to install. In addition, your organization must decide where to host Managed PKI (either locally, or remotely at VeriSign), and which authentication method to use (manual authentication, Passcode Authentication, Registration Authority, or Outsourced Authentication).

Before configuring Managed PKI, your system administrator must first install the hardware components required to support your particular Managed PKI configuration. Once done, a Managed PKI administrator uses the Policy Wizard to configure Managed PKI. For more information on the installation and configuration of Managed PKI, see *Managed PKI Installation and Configuration*.

Note Your original service contract may include assistance from VeriSign's Professional Services Organization (PSO) in the initial installation and configuration of Managed PKI.

Figure 2-3 shows a typical Managed PKI configuration with Local Hosting, Go Secure! for Web Applications, and Registration Authority with key escrow and recovery functionality.

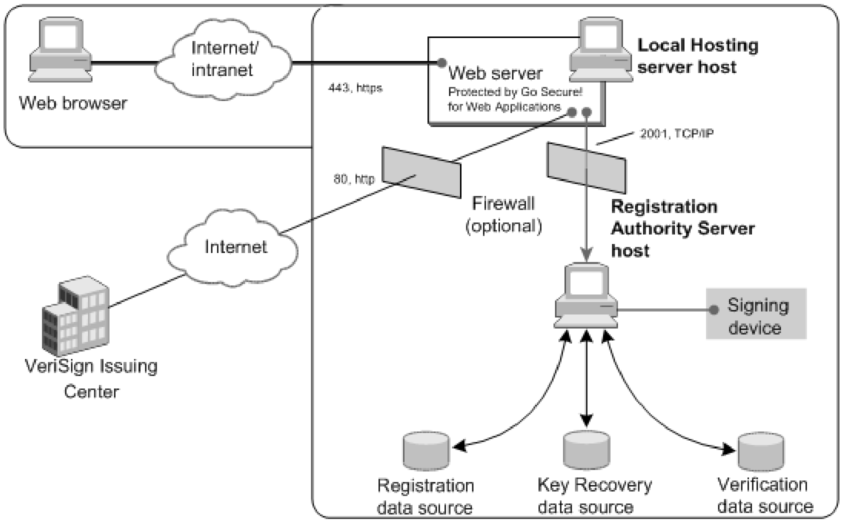

Figure 2-3 Typical Managed PKI configuration

Managed PKI supports intranet, extranet, Internet, VPN, and e-commerce applications. To facilitate secure, large-scale communications and commerce, Managed PKI offers a comprehensive catalog of services and solutions, including:

- Secure Web access
- Local hosting
- Key management and recovery
- Certificate validation
- An application toolkit
- Dual-key support
- Automated certificate renewal

The remainder of this chapter describes the Managed PKI products, configuration options, and optional features. For more information on any of the products, options, and features discussed in this chapter, see the documents described in "VeriSign Managed PKI Documentation" on page 4. For information about the installation and configuration of Managed PKI products, see *Managed PKI Installation and Configuration*, or the relevant documentation for the specific Managed PKI service.

Managed PKI Products

- "Managed PKI Products" on page 14
- "Managed PKI for SSL" on page 15

- "Managed PKI for SSL Premium Edition" on page 15
- "Managed PKI Shared Service Provider (SSP) Option" on page 16

Managed PKI Configuration Options

- "VeriSign Hosting" on page 17
- "Local Hosting" on page 17
- "Manual Authentication" on page 18)
- "Registration Authority" on page 18
- "Outsourced Authentication" on page 20
- "Passcode Authentication" on page 19

Optional Managed PKI Features

- "VeriSign Key Escrow and Recovery" on page 20
- "VeriSign Go Secure! for Web Applications" on page 22
- "Other Go Secure! Services" on page 23
- "Certificate Management Tools" on page 23
- "Managed PKI Premium Validation Services" on page 24
- "LDAP Directory Services Standard" on page 24

Managed PKI Products

VeriSign offers the following Managed PKI products:

- "Managed PKI"
- "Managed PKI for SSL"
- "Managed PKI Shared Service Provider (SSP) Option"

Each Managed PKI product issues and manages a different type of Managed PKI certificate. Although the Managed PKI administrator needs a separate Managed PKI administrator certificate for each product, multiple products can be managed from the same workstation or computer, if desired.

Managed PKI

With Managed PKI, your organization can use certificates to control access to its intranet and extranet. These certificates, known as Digital IDs, identify employees and other affiliates. Issued and managed by your organization, Digital IDs provide network access to authorized parties only. Digital IDs can also provide secure email communication between users. For more information about Managed PKI and Digital IDs, see Chapter 4, "About Certificates."

Managed PKI also enables you to issue and manage Digital IDs for IPSec-compliant devices, routers, and firewalls on your network. IPSec is a framework of open standards designed to secure private communications over IP networks at the network layer. These Digital IDs encrypt and authenticate data sent between these devices, thus creating a secure Virtual Private Network (VPN). Since these Digital IDs work on the network layer, these Digital IDs can also be used to secure communications between company offices, business partners, and remote users over the Internet. This added security eliminates the need for dedicated, leased communications lines and costly, hard-to-maintain modem pools.

Managed PKI for SSL

Managed PKI for SSL allows your organization to provide and manage SSL IDs for servers, while VeriSign performs the back-end public key infrastructure (PKI) functions. The SSL IDs associated with Managed PKI are the standard Internet trust credentials for authenticating Web sites, intranets or extranets, and encrypting information that users exchange online.

Through Managed PKI, individuals in your organization act as the subscribers for the SSL IDs that are then stored in and associated with the servers they manage. The subscribers use the Web-based front-end lifecycle services page to perform activities on behalf of the servers.

For more information about SSL IDs, see Chapter 4, “About Certificates.” For more information about Managed PKI for SSL, contact your VeriSign Account Manager.

Managed PKI for SSL Premium Edition

Managed PKI for SSL Premium Edition provides the more powerful 128-bit Premium SSL IDs.

- **SSL ID.** 40-bit Server ID for client/host authentication and SSL encryption (this certificate will connect at the security level of the browser).

  SSL IDs are issued by the self-signed RSA Secure Server Root, enabling interoperability with most browsers.

- **Premium SSL ID.** 128-bit Server IDs for client/host authentication and SSL encryption (this certificate will cause 40-bit and 56-bit browsers to increase to a 128-bit connection, if capable, while connected to the server).

  Premium SSL IDs are issued by the VeriSign International Server CA which chains up to VeriSign’s Class 3 Primary Certification Authority.

  Intranet SSL IDs are issued by the VeriSign Class 3 Secure Intranet Server CA which chains up to the VeriSign Class 3 Primary Certification Authority.

VeriSign recommends that one SSL ID be used to secure each domain name on every server, even when balancing traffic among several servers for high-traffic sites. VeriSign offers a licensed option for smaller Web farms of identical servers. For more information about Premium SSL IDs, see Chapter 4, "About Certificates." For more information about Managed PKI for SSL Premium Edition, contact your VeriSign Account Manager.

Managed PKI Shared Service Provider (SSP) Option

VeriSign's Shared Service Provider option, which functions under the Federal PKI Policy Authority, enables participants to offer cross-certified CAs for purposes of engaging in business relationships with the Federal government. VeriSign has established an SSP CA that is subordinate to the Federal Common Policy CA, which serves as the "trust anchor" for all certificates issued by VeriSign's SSP CA. The architecture and functional solution for the VeriSign SSP offering is based on VeriSign's Managed PKI service, which has been deployed at numerous government agencies.

VeriSign's SSP option is available for implementation to users with appropriate infrastructure in place. *Managed PKI v7.2 Shared Service Provider Configuration Guide* includes instructions for configuring Managed PKI to issue these certificates. Contact your VeriSign sales representative for more information about SSP and *Managed PKI v7.2 Shared Service Provider Configuration Guide*.

Managed PKI Configuration Options

Before configuring Managed PKI, you should assess which configuration options best meet the needs of your organization. Most importantly, you should consider:

- Who should host the Managed PKI Digital ID Center pages (VeriSign or your organization)
- Which authentication method to use

Subscribers use the Managed PKI Digital ID Center to perform the following certificate lifecycle activities:

- Apply for a certificate
- Track the status of their application for a certificate
- Retrieve their certificate when it is issued
- Locate another subscriber's certificate
- Verify a certificate
- Renew their certificate
- Revoke their certificate

Hosting Options

You can choose to have either VeriSign or your organization host the system. VeriSign hosting offers convenience and quick setup, but hosting it yourself gives you an opportunity to customize and cobrand the Digital ID Center web pages.

VeriSign Hosting

VeriSign hosting offers the simplest and quickest means of implementing Managed PKI. With VeriSign hosting, the Digital ID Center pages are hosted at the VeriSign Issuing Center, rather than on a Web server located at your organization. If you implement Managed PKI with VeriSign hosting, your system is ready to use once you run the Policy Wizard. Although VeriSign hosting is convenient, it does not allow for customizing or cobranding of the Digital ID Center pages.

Figure 2-4 illustrates a typical VeriSign hosting configuration.

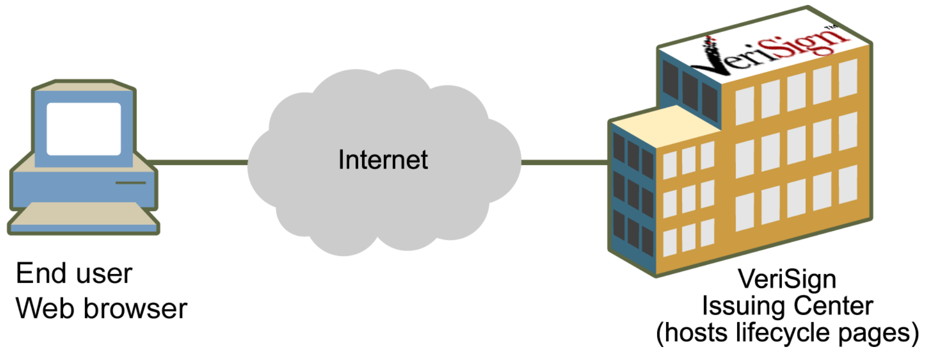

Figure 2-4 VeriSign hosting network

Local Hosting

With Local Hosting, your organization maintains the Digital ID Center pages on your own Web server, rather than storing the pages at VeriSign. Although these pages are hosted locally, certificates are still issued by VeriSign. Local Hosting enables your organization to customize and cobrand the Digital ID Center pages with your own text, links, and/or logo. Local Hosting is required to implement Registration Authority, the optional key escrow and recovery functionality, and Outsourced Authentication. Figure 2-5 illustrates a typical Local Hosting configuration.

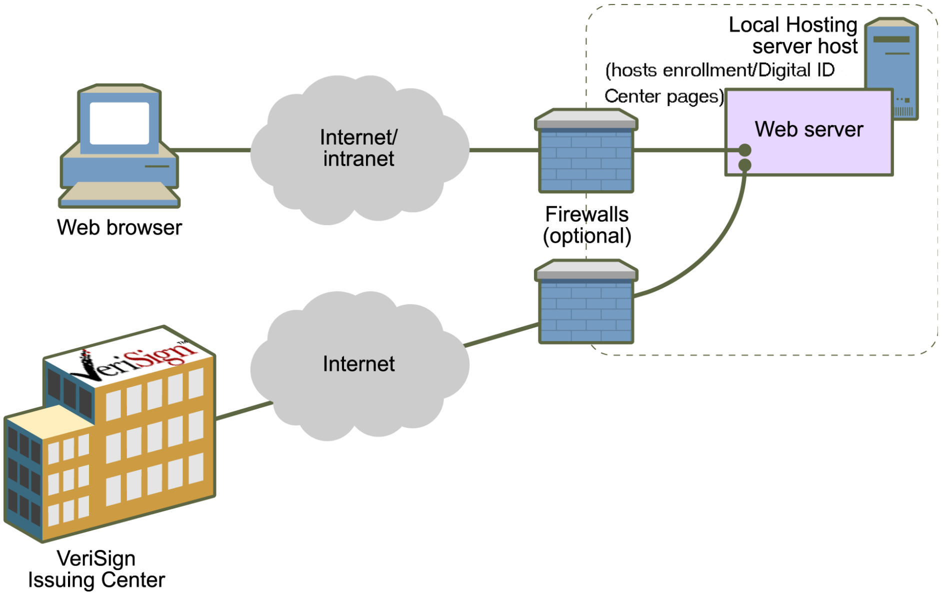

Figure 2-5 Typical Local Hosting network configuration

For more information about Local Hosting, see Chapter , “Understanding Local Hosting” in *Managed PKI 7.2 Technical Reference*.

Authentication Method

Before issuing a certificate, Managed PKI (or the Managed PKI administrator) authenticates the certificate request to determine if it came from an authorized end user and if the request should be approved. Managed PKI offers four methods for authenticating and approving requests: manual authentication, Registration Authority, Outsourced Authentication, and Passcode Authentication.

Manual Authentication

With manual authentication, the administrator personally reviews and approves or rejects each certificate request. Due to the time required of administrators, manual authentication may not be suitable for organizations that issue a high volume of certificates.

Registration Authority

With VeriSign’s Registration Authority option, Managed PKI automatically processes certificate applications without administrator assistance at the time of enrollment. For authentication, Registration Authority compares the enrollment data with preconfigured authentication data stored in an authentication data source (such as your Human Resources database or an LDAP directory). If the applicant is authenticated (that is, if the data matches), the request is approved. Additionally, Registration Authority can be configured to escrow and recover your subscribers’ private keys.

With the Registration Authority API, your software can automatically add data to the approved request. For instance, if management has imposed a spending limit on an employee, the size of the spending limit may be appended to the certificate request. Upon receipt of the request, VeriSign adds the information to the new certificate. Thus, you may completely customize and automate the authentication and issuing process for certificates. Figure 2-6 illustrates a typical Registration Authority configuration.

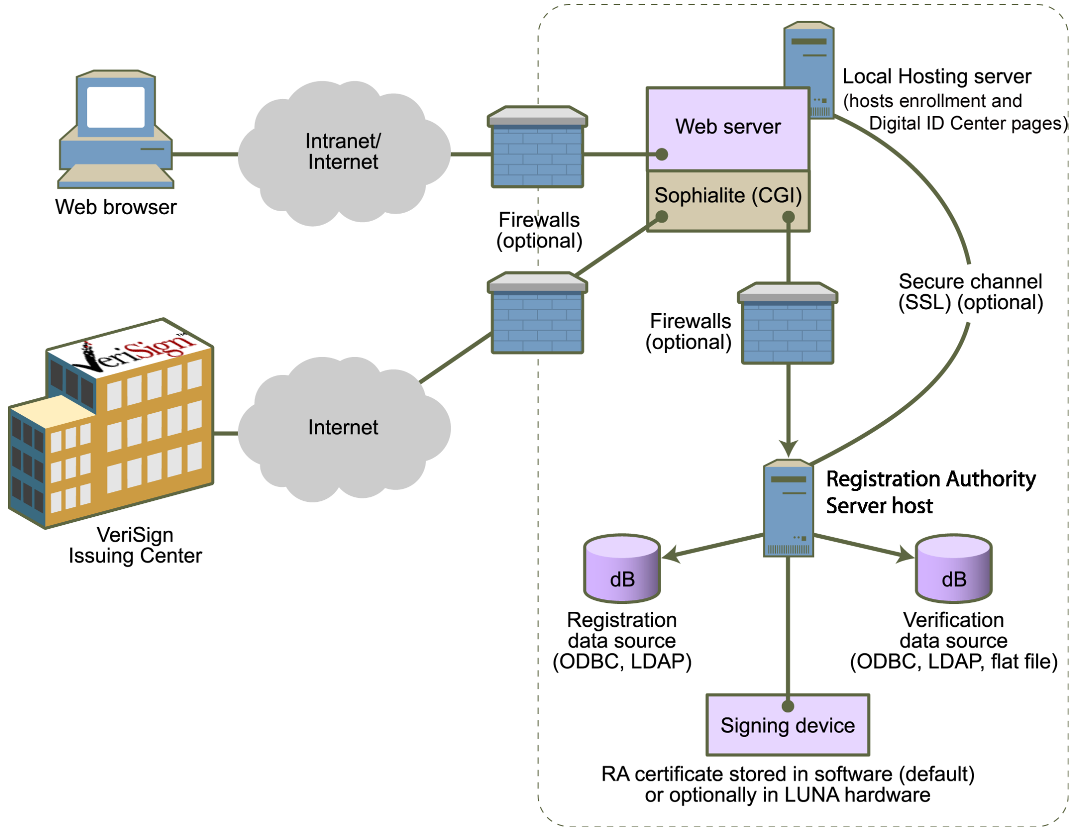
Web browser
Intranet/ Internet
Firewalls (optional)
Local Hosting server (hosts enrollment and Digital ID Center pages)
Web server
Sophialite (CGI)
VeriSign
VeriSign Issuing Center
Internet
Firewalls (optional)
Secure channel (SSL) (optional)
Registration Authority Server host
dB
Registration data source (ODBC, LDAP)
dB
Verification data source (ODBC, LDAP, flat file)
Signing device
RA certificate stored in software (default) or optionally in LUNA hardware

Figure 2-6 Typical Registration Authority network

Unlike manual authentication and Passcode Authentication, Registration Authority requires your organization to establish and maintain authentication servers and Web pages. For more information about Registration Authority, see Chapter , “Understanding the VeriSign Registration Authority Features,” in *Managed PKI 7.2 Technical Reference*. For information about installing Registration Authority, see *Managed PKI Installation and Configuration*.

Passcode Authentication

As with Registration Authority, Passcode Authentication is a service that automatically authenticates certificate requests. However, unlike Registration Authority, Passcode Authentication does not require your organization to establish and maintain authentication servers and Web pages. Instead, all authentication software and support is provided by VeriSign. As a result, Passcode Authentication is easier to implement but slightly less flexible than Registration Authority.

The administrator configures Passcode Authentication through the Control Center. When a subscriber applies for a certificate, the enrollment information is securely uploaded to VeriSign and compared to information previously provided by the administrator. Depending upon the approval guidelines established by your organization, the certificate request is either approved or rejected.

With Passcode Authentication, your organization need not provide any additional programming or hardware. All certificate generation and maintenance operations are hosted at VeriSign's secure Web site, thereby relieving your organization of the time and expense of creating and supporting certificate authentication solutions.

For more information about Passcode Authentication, see Chapter , "Understanding Passcode Authentication," in *Managed PKI 7.2 Technical Reference*. For information about installing Passcode Authentication, see *Managed PKI Installation and Configuration*.

Outsourced Authentication

Outsourced Authentication (OA) enables your organization to outsource some or all of its authentication processes to VeriSign's Business Authentication Service. Outsourced Authentication uses a customized version of Automated Administration to perform the authentication within your organization. Applicants you know are approved based on parameters determined by your organization, and applicants you don't know are authenticated by VeriSign.

With OA, the Business Authentication Service is responsible for verifying the existence, name, and authorization of parties requesting certificates. However, if desired, your organization may retain the authentication tasks for *known* applicants—those who either already have certificates, or those who meet criteria defined by your organization. You decide how much of the authentication process to assign to VeriSign.

Outsourced Authentication customers receive *Outsourced Authentication Administrator's Guide* as part of their documentation set. For more information about Outsourced Authentication, contact your VeriSign Account Manager.

Optional Features

To enhance the capabilities of the Managed PKI products, VeriSign offers a number of optional features, described below.

VeriSign Key Escrow and Recovery

VeriSign Registration Authority includes an optional key escrow and recovery system. In addition to automatically approving certificate enrollment requests, the key escrow and recovery functionality enables your organization to:

- Generate keys in a secure central location
- Deliver keys to subscribers
- Securely hold personal keys in an encrypted database (for key recovery)
- Maintain secure records of key history
- Recover private keys, as needed

With key escrow and recovery, keys can be generated locally by the browser (distributed key generation), or centrally by the Registration Authority server (centralized key generation). Both distributed and centralized key generation offer distinct advantages. For example, distributed key generation improves nonrepudiation, but requires more of the user's time in the issuing process. With both methods, the private keys are never seen by VeriSign.

Over time, a subscriber will use different key pairs (for instance, key pairs may be reissued every year). Therefore, old private keys may be needed to decrypt old encrypted files. For this reason, the key escrow feature maintains a key history for each subscriber, and provides the ability to recover old keys if they are lost or withheld by an incapacitated or uncooperative user.

Dual Key Pair Option. With the Dual Key Pair option of key escrow and recovery, your organization benefits from the advantages of both centralized and distributed key generation. In a dual key pair system, one key pair is centrally generated and stored, while another key pair is generated and stored within each user's browser. Accordingly, the end user receives two Managed PKI Digital IDs. The centrally generated private key and certificate are used for client authentication, as well as data encryption and decryption. The other private key and certificate are used only for signing.

Single Key Pair Option. With the Single Key Pair option of key escrow and recovery, the subscriber receives a single key pair and certificate. This key pair/certificate can be used for signing, client authentication, and data encryption (all uses).

Figure 2-7 illustrates a typical Registration Authority configuration with key escrow and recovery functionality.

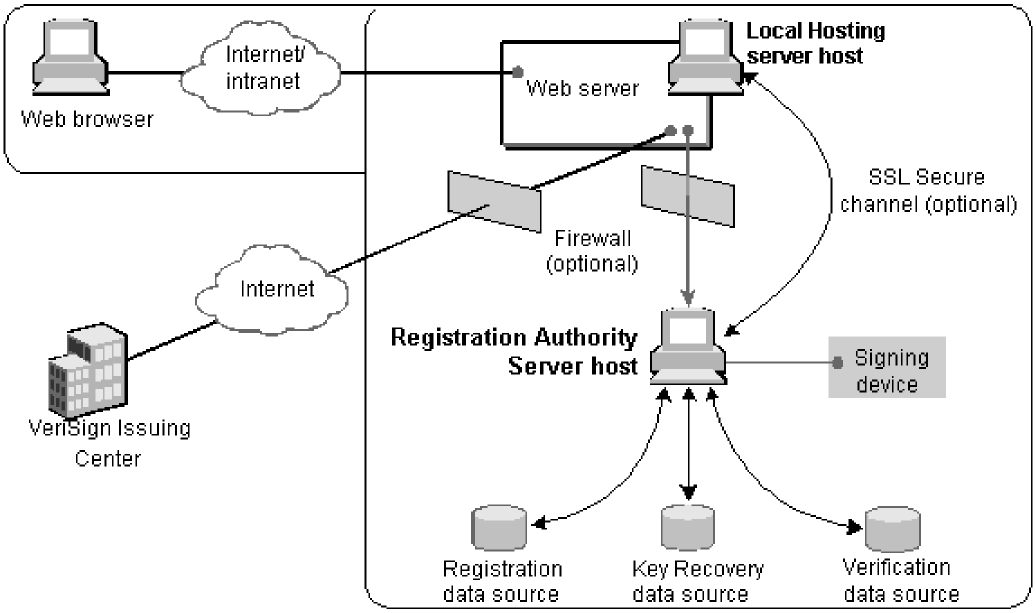

Figure 2-7 Registration Authority with key escrow and recovery functionality

For more information about key escrow and recovery, see *Managed PKI Key Escrow and Recovery Guide*. For information about configuring key escrow and recovery, see *Managed PKI Installation and Configuration*.

VeriSign Go Secure! for Web Applications

VeriSign's Go Secure! services are designed to enhance the security of transaction and communication applications. Go Secure! for Web Applications makes it easy to secure your Web-based applications.

VeriSign Personal Trust Agent

A component of Go Secure! for Web Applications, VeriSign's Personal Trust Agent (PTA) equips Web applications with subscriber authentication, transaction signing, and access control. Rather than using the native SSL-based subscriber authentication in browsers and servers, the PTA implements its own subscriber authentication. With PTA subscriber authentication, you may develop more user-friendly Web access control systems. VeriSign also provides a generic CGI front end that you can use to develop support for transaction verification with any Web server that supports SSL. If you use Go Secure! for Web Applications in conjunction the VeriSign Roaming Service, the certificates are available from any browser.

Other Go Secure! Services

In addition to Go Secure! for Web Applications, VeriSign offers a continually expanding selection of Go Secure! services. Each Go Secure! service comes with its own administrator's guide. The administrator guides explain the requirements, configuration process, and operation of each Go Secure! service.

An example of the other Go Secure! services offered by VeriSign is **VeriSign Go Secure! for Microsoft Exchange**. Designed for use with Microsoft Exchange servers, Go Secure! for Microsoft Exchange enables subscribers to exchange digitally signed and encrypted email within your organization. By integrating Managed PKI with the Exchange user directory, Go Secure! for Microsoft Exchange also automatically updates your organization's directory of certificates.

For more information about Go Secure! products, see your Account Manager or see the appropriate Go Secure! documentation.

Certificate Management Tools

Two certificate management tools are provided with Managed PKI: the VeriSign Certificate Parsing Module (CPM) and the VeriSign Certificate Validation Module (CVM). Typically, these modules are used in conjunction with a Web server that is using native client authentication. Although CPM and CVM are installed automatically with Go Secure! for Web Applications, they may be used independently of Go Secure! for Web Applications.

VeriSign Certificate Parsing Module

The VeriSign Certificate Parsing Module (CPM) is a software suite that extracts fields from certificates presented to a Web server. CPM then presents the extracted information to certificate-enabled applications.

VeriSign provides two CPM implementations:

- Server plug-in version (NSAPI or SAF)
- Programmer's library version — shared-object (.so) file for UNIX systems, and a dynamic-linked-library (.dll) in Microsoft Windows WIN32 systems.

For most Managed PKI implementations, VeriSign recommends the server plug-in version because it features a simpler interface and upgrade process. The server plug-in is compatible with other server plug-ins, as well as extensions such as servers, JavaScript, CGI programs in any programming language (csh, Perl, C, C++), and NSAPI modules. For more information about CPM, see *Managed PKI v7.2 Certificate Validation Module*.

VeriSign Certificate Validation Module

On a regular basis, VeriSign updates and releases a certificate revocation list (CRL) for each of its Certification Authorities. Before trusting a certificate, server software must check the corresponding CRL to ensure that the certificate has not been revoked.

To automate the CRL-checking process, VeriSign's Certificate Validation Module (CVM) provides ready-to-use Web server plug-ins. CVM includes plug-ins for popular Web servers, as well as a programmer's interface for developing custom applications. For more information about CVM, see *Managed PKI v7.2 Certificate Validation Module*.

Managed PKI Premium Validation Services

In its role as a Certification Authority, VeriSign provides certificate revocation information in several forms:

- Real-time validation through Online Certificate Status Protocol (OCSP) services and XKMS Validation Services
- Hourly certificate revocation list (CRL) generation

Managed PKI Real Time Validation Service - OCSP

Managed PKI Real Time Validation Service - OCSP enables you to validate certificates through OCSP. Applications may automatically determine the revocation status of a certificate. Revocation statuses include *valid*, *revoked*, *suspended*, *expired*, or *unknown*. For OCSP, when a user presents a certificate to a Web server or other network resource, CVM requests the certificate status from the Certification Authority. If the status is *valid*, the user can access the resource. If the status is *revoked*, *suspended*, *expired,* or *unknown*, the user cannot access the resource.

Premium CRL Service

With Premium CRL Service, VeriSign updates CRLs hourly, rather than daily. When a user presents a certificate to a Web server or other network resource, an application may check the certificate against the CRL. If the certificate is listed as *revoked*, the user cannot access the resource. If the certificate is not listed, the user can access the resource.

LDAP Directory Services Standard

VeriSign is committed to full support of the Lightweight Directory Access Protocol (LDAP) directory services standard. Managed PKI supports export of our certificate information into any directory service that complies with the standard. Optionally, you can manually export your directory data from VeriSign's central repository for import into nonstandard applications.

Enrolling For Managed PKI

This chapter explains how to enroll your organization for Managed PKI, and how to enroll yourself as a Managed PKI administrator. This chapter includes the following topics:

Make These Decisions Before Enrolling

This section summarizes the decisions you should make before enrolling for Managed PKI.

Choose Contact Personnel

The Managed PKI enrollment form requires that you assign three roles for your organization: the Organizational Contact, the Administrator, and the Billing Contact. While the same person may assume one or more of these roles, you should assign these roles before enrolling for Managed PKI.

- **Organizational Contact:** The organizational contact is your company representative who is authorized to sign a binding agreement for Managed PKI service. Typically, the organizational contact is a high-level manager.
- **Administrator**: The administrator is the person responsible for managing your Managed PKI service. The administrator authenticates, approves, and rejects certificate requests. The administrator can also revoke subscriber certificates. Typically, an organization will appoint its IS manager, a Human Resources representative, or a security/badging officer as its administrator. If desired, your organization may appoint more than one administrator. Once you have enrolled for Managed PKI, you may enroll additional administrators by accessing one of the following URLs:

- For Pilot Managed PKI: **https://pilotonsite.verisign.com/OnSiteServiceEnrollAdditional.htm**
- For Production Managed PKI: **https://onsite.verisign.com/OnSiteServiceEnrollAdditional.htm**

+ **Billing Contact**: The Billing Contact is the person responsible for the payment of Managed PKI services. In addition, the Billing Contact notifies VeriSign of any billing-related changes or developments. Typically, an organization will appoint its Finance and Accounting Officer, or an accounts payable representative, as its Billing Contact.

Decide Between Public and Private Certification

When your organization enrolls for the Managed PKI Service, you will specify whether your certificates are issued under a private CA—your organization—or by a public CA in the VeriSign Trust Network. Since your decision to use a public or private CA cannot be changed, carefully consider the advantages of both options.

+ **Public Certification**: Public certificates reside in the VeriSign Trust Network (VTN), a globally interoperable digital certificate infrastructure based on a trusted network of Certification Authorities throughout the world. The roots of the VeriSign Trust Network are embedded in all popular browsers, servers, and email packages. Therefore, public certificates can be used across organizations without any special preparation on the part of certificate users.

  With public certification, you do not have to distribute your root to all potential message recipients. Instead, email sent by users will automatically be trusted by the recipient's email applications. Therefore, if you plan on using certificates for email outside of your organization, you should use public certification. All public certificates have liability coverage under VeriSign's NetSure Protection Plan.

  Note If you select the public CA option, your organization must adhere to VeriSign's Certification Practice Statement (CPS). Organizations running a Public Certificate Authority are responsible for verifying the identity of certificate applicants, as described in the CPS. To view the CPS, see: **https://www.verisign.com/cps**.

+ **Private Certification**: Unlike public certificates, private certificates do not reside in the VeriSign Trust Network. Instead, your organization establishes a separate hierarchy with its own root at the top.

  Generally, private certificates are used within your organization for applications such as intranets, virtual private networks (VPNs), and, occasionally, for Web access. Although private certificates may also be used externally in private domains, they require that you first distribute your organization's root and certificates to those with whom you wish to communicate. Browser administration kits are available from Netscape and Microsoft to assist with this task.

Organizations running a private CA are responsible for defining and following their own authentication procedure for verifying the identity of certificate applicants. Also, certificates in the private key hierarchy are not protected under VeriSign's NetSure Protection Plan.

- If you plan to issue certificates to nonentities, or you do not plan to use a strong authentication method on your users, then you should use private certification.
- If you are implementing IPSec, you must use private certification.
- If you plan on using certificates to send email outside of your organization, VeriSign recommends that you not use a private certification.

For further information about CAs, see *Managed PKI v7.2 Administrator's Handbook*.

Decide How Many Certificates You Need

When you enroll for the Managed PKI Service, you must specify the number of certificates that you wish to obtain for your organization. As you increase the quantity of certificates ordered, the price per certificate decreases. When you purchase Managed PKI for multiple applications, VeriSign charges for certificates on a per-seat basis. At any time, you can purchase additional certificates by clicking *Support and Services* in the top banner of the Control Center.

Decide Whether To Use CSR-based Enrollment

Managed PKI offers two options for certificate enrollment: browser-based enrollment and CSR-based enrollment. A CSR, or Certificate Signing Request, is a machine-readable version of a certificate request.

With browser-based enrollment, the browser generates the public/private key pair for each applicant. Applicants then acquire their certificates through the Web. Browser-based enrollment does not require any changes to your Managed PKI configuration.

If your application cannot use a browser, CSR-based enrollment provides the simplest method of enrolling for certificates. With CSR-based enrollment, an application other than the browser generates the key pairs. In such cases, the public key is extracted from the CSR file generated by the application. Applicants paste the CSR into a Web-based enrollment form and receive the certificate by email. Once received, the certificates need to be installed in the application.

CSR-based enrollment is useful for issuing certificates to nonstandard or custom applications. However, you should only employ CSR-based enrollment if you have an application other than a browser or email application that uses certificates. In addition, the application must be able to produce CSRs.

Note VeriSign provides a browser emulation specification that enables non-browser applications to use browser-based enrollment. For more information, see the *Managed PKI 7.2 Technical Reference*.

To configure Managed PKI for CSR-based enrollment, run the CSR Enrollment Wizard from the Control Center *Configuration* page. CSR-based enrollment can be configured at any time and may be used in tandem with browser-based enrollment.

Note Managed PKI for SSL uses CSR-based enrollment by default.

Understand Your Responsibilities

Read *Managed PKI Administrator's Handbook* and *Managed PKI Getting Started*

Managed PKI v7.2 Administrator's Handbook provides a comprehensive overview of your responsibilities as an administrator. The appendices in *Managed PKI v7.2 Administrator's Handbook* provide information to assist you in meeting the requirements of the VeriSign Certification Practice Statement (CPS). This documentation is available on the VeriSign Managed PKI CD. Once your organization has enrolled for Managed PKI, you may access the Handbook by clicking the **Documentation** link on the *Download* page of the Control Center.

Managed PKI v7.2 Getting Started provides information on setting up your organization to run a public key infrastructure using VeriSign's Managed PKI. It provides information on implementing Managed PKI within your organization and rolling out Managed PKI Digital IDs to your end users.

System Requirements

To prepare for your implementation of Managed PKI, your organization should complete the requirements outlined in *Managed PKI Installation and Configuration*, and *Managed PKI v7.2 Hardware/Software Requirements*.

Create an Authentication Process (for Public Certification only)

As the CA for all public certificates, VeriSign relies upon administrators to properly authenticate certificate applications. To develop and implement a compliant certificate authentication process, you should first review *Managed PKI v7.2 Administrator's Handbook*.

Managed PKI v7.2 Administrator's Handbook explains the certificate lifecycle within VeriSign Public Certification Services (PCS). Since you will be approving the issuance of certificates within the VeriSign PCS, you must adhere to the applicable requirements of the Certification Practice Statement (CPS).

Prepare to Support Subscribers

As an administrator, you will serve as the primary Managed PKI technical support agent for your organization. To assist you in supporting your subscribers, VeriSign has developed the following online resources:

- Subscriber User Manual: **http://www.verisign.com/client/guide/index.html**
- IPSec ID FAQ: **http://www.verisign.com/onsite/ipsec/ipsecFaq.html**
- Digital ID Center Help Desk at **http://www.verisign.com/client/help/index.html**
- Online copies of Managed PKI documentation from the Download page of the Managed PKI Control Center.

Note To view VeriSign's online documentation, you must have Adobe Acrobat Reader on your system.

Reference materials for Managed PKI products are posted on VeriSign's Web site. To answer questions from your subscribers, you may refer to this documentation. In addition, you may copy and paste information from the documentation into your email responses to their questions.

In addition to Managed PKI documentation and online resources, you may want to learn more about certificate technology, in general:

- *Secure Electronic Commerce*, Warwick Ford, Michael Baum, Prentice Hall, 1997.
- VeriSign's **http://www.verisign.com/resources/wp** and **http://www.verisign.com/**.

Select Good Passwords

When picking passwords, choose something that cannot easily be guessed. A good password is typically a minimum of six to eight characters long, and consists of upper- and lower-case letters and numbers.

Test Drive Managed PKI

To familiarize yourself with Managed PKI, you may download the Evaluation Edition of Managed PKI. With the Evaluation Edition of Managed PKI, you can explore Managed PKI functions and configuration options. For supporting documentation, see the *Download* page in the Evaluation Edition's Control Center. VeriSign strongly recommends that you run the Evaluation Edition.

Note The Evaluation Edition of Managed PKI is free-of-charge and entails no obligation.

You can access the Evaluation Edition at **http://testdrive.verisign.com**.

Applying for an Administrator ID

You will need an administrator ID to access the Control Center. To sign up for Managed PKI, contact your VeriSign account representative, or follow the steps given here.

Note The order of these steps may vary slightly depending on the Managed PKI service for which you enroll.

1 Open **https://onsite.verisign.com/** and select the Managed PKI service you wish to purchase.

2 Enter your Company, Department, or Agency Information. Provide the name and contact information for your organizational contact, the person within your organization who is responsible for the VeriSign Managed PKI service, for providing organizational information, and who is authorized to activate the CA on behalf of your organization. VeriSign uses this information in the public key of your administrator ID.

   To avoid confusion at a later time, enter clear and distinct terms in the **Company/Department/Agency** and **Department/Organization/Project** fields.

   Note You must use the legal business name of your organization. VeriSign will verify your authorization to use this name.

3 *Enter Administrator Information*. Provide the name and contact information for your administrator. If the administrator and organizational contact are the same person, select **Same as Organizational Contact**.

4 *Enter a Challenge Phrase*. In the **Challenge Phrase** and **Reconfirm** fields, enter a challenge phrase. Your challenge phrase is the password you will use to pick up your administrator ID. Since you may need the challenge phrase to replace your administrator ID in the future, enter a memorable phrase. Only you have access to your challenge phrase, so please save it in a safe place.

   Note The **Challenge Phrase** and **Reconfirm** fields are case-sensitive.

5 *Enter the DNS Domain Names for your Digital IDs (for IPSec, SSL IDs, and Premium SSL IDs only)*. Enter the domain names for which you want to issue certificates. Your organization must be the registered owner of these domain names.

   For IPSec (VPN) accounts, the domain name is optional, unless:

   + The device is made by Cisco, or

+ Your enrollment process requires a domain name to direct enrollments to the proper CA

6 *Choose the Number of Subscriber Certificates.* Select the number of end user certificates you wish to purchase.

7 *Enter Billing Contact Information.* Provide the name and contact information for your billing contact. If the billing contact is the same person as the administrator or organizational contact, select the appropriate radio button.

8 *Choose the Payment Method for Your VeriSign Managed PKI Service.* Select your payment preference, and enter the appropriate information.

9 *Enter Your D-U-N-S Number.* Enter your Dun & Bradstreet number. If you do not already have a D-U-N-S number, click the link and apply for one.

10 *Choose a Nonstandard Certificate Authority Name (for Private Managed PKI and VPN/IPSec services only).* If you have chosen to purchase VeriSign Managed PKI using a Private Certificate Authority (CA), VeriSign will create a CA specifically for your organization based on the information you have provided and our expertise in public key infrastructure. If you would like to request specific CA requirements, check the **Contact me about the design of my Certificate Authority** box.

11 *Carefully Read the Subscriber Agreement.* Governed by VeriSign's Certification Practice Statement (CPS), the Subscriber Agreement is a legally binding contract. Therefore, you should read the Subscriber Agreement carefully before proceeding. To review the CPS, click the **VeriSign Certification Practice Statement** link.

12 Accept or decline the Subscriber Agreement.

To accept the Subscriber Agreement, click **Accept**. Do not interrupt your browser while it processes the enrollment, or you will have to repeat the application process.

If you do not agree to the terms of the Subscriber Agreement, click **Decline**, and the certificate application will be terminated. You cannot obtain a certificate if you decline the Subscriber Agreement.

If you completed the enrollment page correctly, the *Managed PKI Enrollment Complete* page appears. This page contains contact information and links for **Documentation** and **Payment**. Shortly, you will receive an email from VeriSign containing instructions for completing your application.

Note The Common Name is an attribute value within the Distinguished Name of a certificate. For SSL IDs and Premium SSL IDs, the Common Name is the DNS host name of the site to be secured. For end-user IDs, the Common Name is typically the subscriber's first and last names. For IPSec Digital IDs, the Common Name is a concatenation of the first and last name on the account.

13 Once you complete your application, make arrangements for payment.

When VeriSign approves your enrollment, you will receive another email message from VeriSign. This email message contains a URL and a personal identification number (PIN).

14 To pick up your certificate, open the URL, and then type the PIN and your challenge phrase.

Note If you choose to store the administrator certificate on a USB token, VeriSign provides an optional Administrator Kit containing an Aladdin USB token, cable connector, and software. You must install this reader before picking up the administrator certificate. See *Managed PKI Installation and Configuration* for instructions on installing the Administrator Kit.

15 Select the Cryptographic Service.

+ *For Microsoft Internet Explorer*: If you wish to store the private key on your computer, you can choose either the Base CSP (40-bit session key strength) or the Enhanced CSP (128-bit session key strength) from the drop down list. (VeriSign recommends always choosing the strongest available CSP.)

  If you have a USB token, choose a service provider from the drop-down list.

+ *For Netscape Navigator*: If you have a USB token, enter a password in the dialog box that appears during download.

  If the USB token software is not properly installed, you see instead a dialog box that requests a password for Communicator Certificate Database. If you proceed, the administrator certificate downloads to the Netscape Communicator Database. Netscape has an export/import feature that allows you to import the certificate to the USB token at a later time, when the USB token is installed correctly.

16 Additional Security for Your Private Key (For Microsoft Internet Explorer only). VeriSign recommends that you protect the private key associated with your administrator ID by checking the box on the bottom of the page. This allows you to protect your private key with a password.

17 Once you have completed the fields on this page, click **Accept**, and then follow the instructions to install the administrator ID.

Note If you need a backup copy of your administrator ID, download the certificate to a directory (rather than installing it in your browser or on a USB token). Once you make your backup copy, install the original certificate manually, according to the security instructions for your browser or USB token.

18. Once you have installed the administrator ID, go to the Control Center at **https://onsite-admin.verisign.com/welcome.htm**. If you have stored the administrator ID on a USB token, ensure the USB token is firmly inserted in the reader.

    The first time you access this Web site, the *Welcome To VeriSign Certificate Services* page appears. This page contains a brief overview.

19. Read the overview, and click **Continue**.

    The *Choose Your Digital ID Type* page appears. VeriSign customizes this page to reflect the type of certificate you purchased.

20. Click the appropriate hypertext link. The Policy Wizard page appears.

    To configure Managed PKI with the Policy Wizard, see *Managed PKI Installation and Configuration*.

Checklist for Becoming an Administrator

Use the following checklist to ensure that you are prepared to enroll as an administrator.

Table 3-1 Administrator enrollment checklist

Task	**Done?**
Make These Decisions Before Enrolling:	
▪ Choose Contact Personnel	
▪ Decide Between Public and Private Certification	
▪ Decide How Many Certificates You Need	
▪ Decide Whether You Will Use CSR-based Enrollment	
Download Adobe Acrobat Reader so that you will be able to read online documents	
Understand Your Responsibilities:	
▪ Read *Managed PKI v7.2 Administrator's Handbook* and *Managed PKI v7.2 Getting Started*	
▪ Ensure That You Have the Correct Hardware and Software	
▪ Ensure That Subscribers Have the Correct Software	
▪ Create an Authentication Process (If You Choose Public Certificates)	
Prepare to Support Subscribers by reading the Online Resources	

Table 3-1 Administrator enrollment checklist (Continued)

Task	Done?
If using passwords, establish and communicate a password policy	
Test Drive Managed PKI	
Learn More about Certificate Technology	
Apply for an Administrator’s Certificate	

About Certificates

A digital certificate, or Digital ID, provides a means of proving an identity in electronic transactions—much like a company badge or passport does in face-to-face interactions. Certificates can be used for a variety of electronic transactions including email, secure Web access, electronic commerce, groupware, and electronic funds transfers. Chapter 2, "About Managed PKI," describes the function and benefits of certificates in Managed PKI. This chapter discusses certificates in further detail.

For more information about issuing and managing Managed PKI certificates, see *Managed PKI Administrator's Handbook*.

This chapter includes the following topics:

- "Why Can I Trust a Certificate?" on page 35
- "Types of Certificates" on page 38
- "Issuing Certificates with Managed PKI" on page 41

Why Can I Trust a Certificate?

A Certification Authority (CA) is an entity that issues, manages, revokes, and renews certificates. Upon issuance to a subscriber, a certificate is digitally-signed by a CA. VeriSign owns and operates CAs. The CAs can be within the VeriSign Trust Network (VTN) or outside of the VTN. The VTN is a globally interoperable digital certificate infrastructure including CAs throughout the world. If you choose to have your CA outside of the VTN, your organization may operate its own CA.

Certificates contain the following information (see Figure 4-1):

- Subject identification information, including the Distinguished Name of the subscriber. A Distinguished Name (DN) is a set of data that uniquely identifies an entity, such as a person. For example, the Distinguished Name for John Doe might include the following data:

  country=US
  state=California
  organizationName=Your Company, Inc.
  commonName=John Doe

- Public key of the subscriber
- Validity period for the certificate (the time period between the issuing and expiration of a certificate)
- Name and digital signature of the Certification Authority that issued the certificate
- Certificate Serial Number

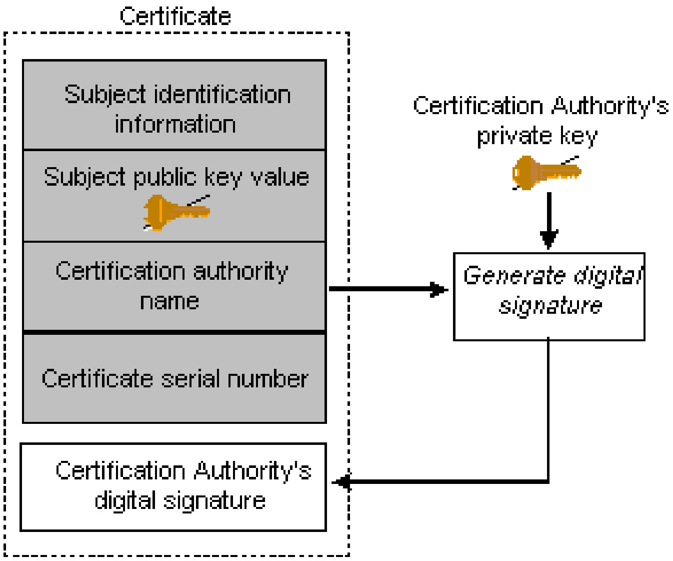
Certificate
Subject identification information
Subject public key value
Certification authority name
Certificate serial number
Certification Authority's digital signature
Certification Authority's private key
Generate digital signature

Figure 4-1 The structure of a certificate

When a subscriber sends a digitally-signed message, the application attaches a copy of the public key portion of their certificate to the message. The sender's private key is then used to digitally sign the certificate. When the recipient receives the message from the sender, he or she uses the sender's public key to verify the digital signature. If the public key matches the digital signature, then the recipient can be confident that the message originated with the sender and that the message was not altered in transit. In short, digital signatures authenticate the identity of the subscriber, just as your name and photograph authenticate your identity on your driver's license.

Figure 4-2 illustrates the structure of a public certificate signed by a Certification Authority.

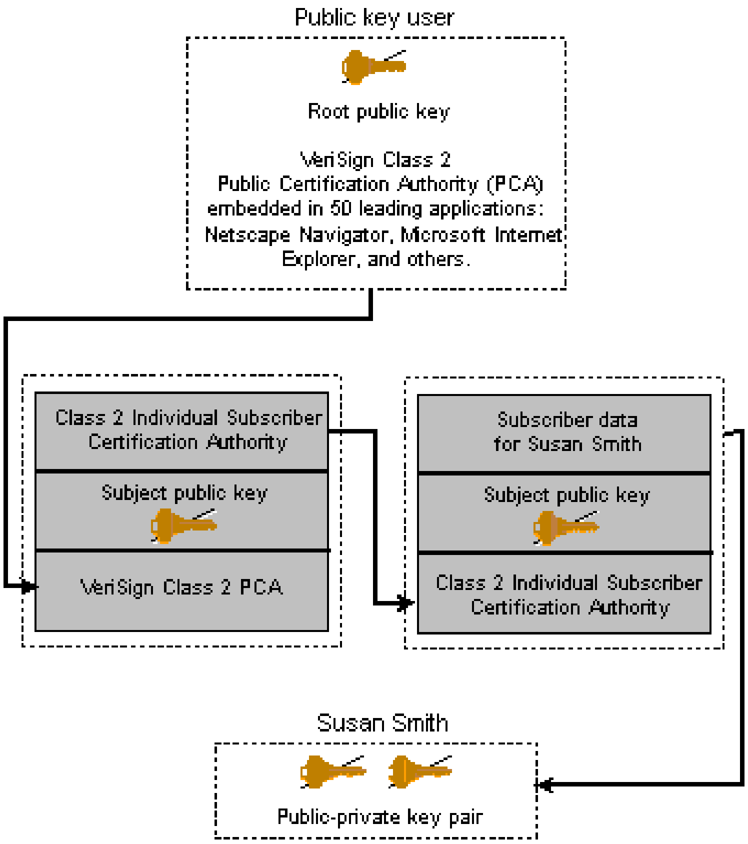

Figure 4-2 The structure of a public certificate signed by a Certification Authority

VeriSign offers three levels of assurance and trust within the VeriSign Trust Network public hierarchy:

- Class 1 certificates provide the lowest level of assurance and trust. Class 1 certificates only validate the email address of the individual to whom the certificate was issued.
- Class 2 certificates offer a median level of assurance and trust. Class 2 certificates use an online consumer database and mail-back verification to validate the identity of the individual to whom the certificate was issued.
- Class 3 certificates offer the highest level of assurance and trust. For validation, Class 3 certificates require individuals to physically present proof of identity to an authorized agent. To validate organizations, Class 3 certificates use business databases (such as Dun & Bradstreet) and independent callbacks.

VeriSign also supports private hierarchies in which the CAs reflect the customer's company name and are not part of the VeriSign Trust Network.

Types of Certificates

Managed PKI offers the following types of certificates:

- Digital IDs
- SSL IDs
- Premium SSL IDs

Digital IDs

A Digital ID uniquely identifies a person or a computer device. Digital IDs enhance privacy by encrypting subscriber email communications and interactions with Web sites. Digital IDs can be used to limit access to a Web site, or to enhance the security of email messages.

Figure 4-3 illustrates the following processes for Digital IDs:

- Signing an email message — Vera uses her private key to digitally sign a message. All signing is done by the sender.
- Authenticating an email message — All authentication is done by the recipient. John uses Vera's public key to confirm that the message was indeed sent by Vera. John also verifies that the message was not altered by an unauthorized party in transit.

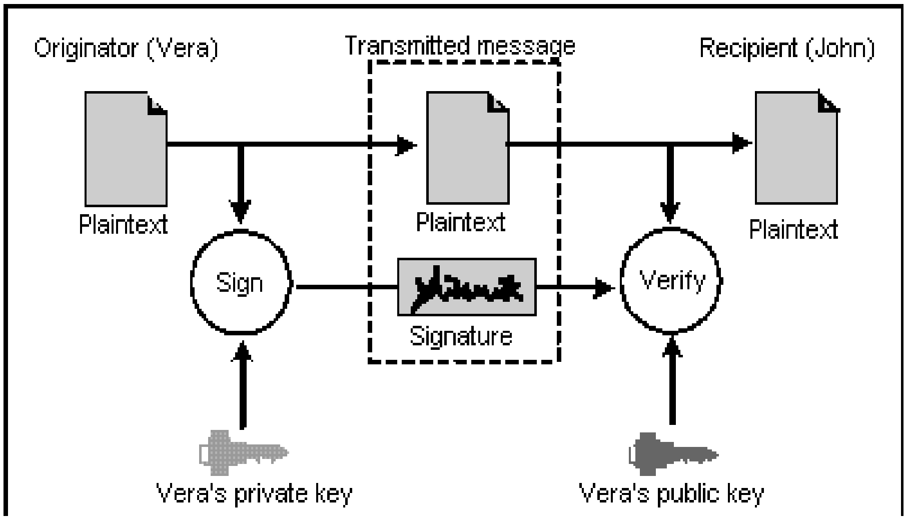

Figure 4-3 Signing and authenticating an email message with a Digital ID

IPSec Digital IDs

Digital IDs can also be configured to identify and authenticate remote access users to devices, such as firewalls or routers. IPSec Digital IDs identify and authenticate a hardware device that uses the IPSec (IP Security) protocols for secure communications. The IPSec protocols provide for the secure exchange of IP packets. Unlike SSL, which works at the application layer, IPSec encrypts the IP packets at the IP network layer. IPSec Digital IDs can be used to implement Virtual Private Networks (VPNs), secure extranets, and remote user access.

IPSec Digital IDs are used for the authentication and encryption of data passed between two network peers, such as two routers. Working within the existing Internet infrastructure, IPSec Digital IDs encrypt the contents of each outgoing IP packet. Although the contents are encrypted, the packet retains the IP format. The packet is then marked for delivery to the intended IPSec-compliant receiving device. Upon receipt, the receiving device unpacks and decrypts the packet.

SSL IDs

An SSL ID identifies a secure Web server. With SSL IDs, subscribers can confirm the identity of a Web server to which they connect. To secure Web server communications, SSL IDs use Secure Sockets Layer (SSL) technology. Data transferred over a secure SSL connection between a client and a server can be encrypted and decrypted.

SSL IDs are useful for individuals engaged in financial transactions, as well as businesses sending classified information. Netscape and Microsoft Web servers and browsers support SSL, and many Web sites use SSL to transfer confidential information. By convention, Web pages that require an SSL connection start with “https:” instead of the more common “http:”.

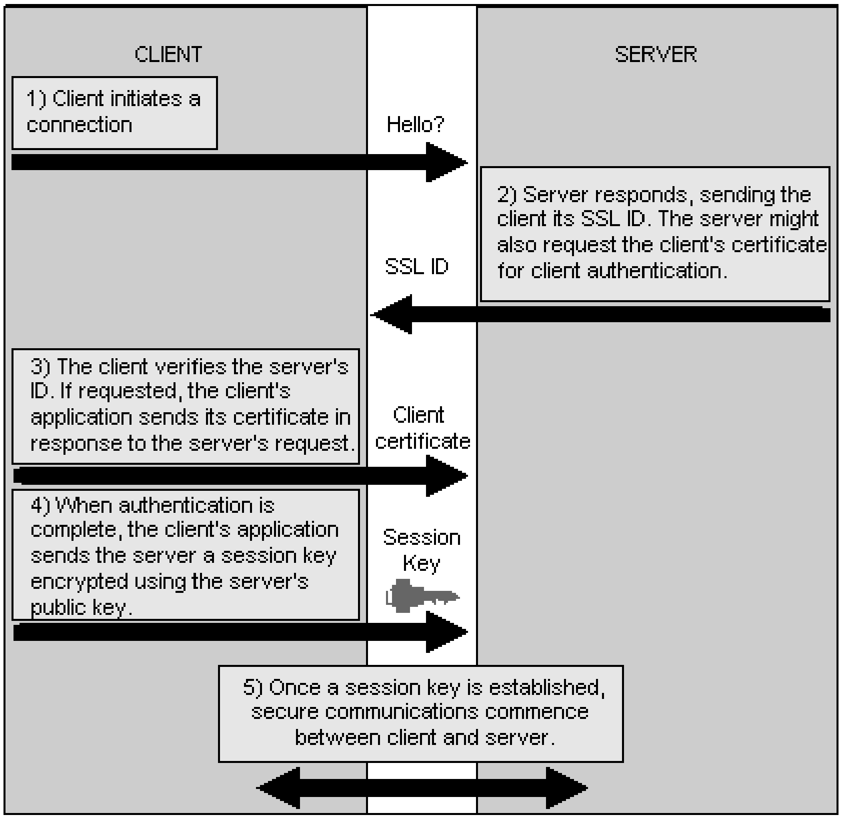
CLIENT
SERVER
1) Client initiates a connection
Hello?
2) Server responds, sending the client its SSL ID. The server might also request the client's certificate for client authentication.
SSL ID
3) The client verifies the server's ID. If requested, the client's application sends its certificate in response to the server's request.
Client certificate
4) When authentication is complete, the client's application sends the server a session key encrypted using the server's public key.
Session Key
5) Once a session key is established, secure communications commence between client and server.

Figure 4-4 SSL communication using Managed PKI for SSL and client Digital IDs

Figure 4-4 illustrates the encryption and authentication of communications using SSL IDs and the SSL protocol. All transactions occur automatically, without intervention from the client's application.

1. When the client encounters a Web server page configured for SSL, the client requests the SSL ID from the server.
2. The server sends its SSL ID to the client. The SSL ID was signed by the private key of the CA when it was issued. If the server needs to confirm the client's identity for access authorization, it requests a copy of the client's certificate.
3. The client's application uses the CA's public key to validate the SSL ID. The client's application then compares the fully-qualified domain name of the site to the fully-qualified domain name listed in the SSL ID. If the information matches, the client may be confident that it is communicating with a site that has been fully authenticated according to the CA's policies and practices.
4. Once the server's identity has been authenticated, the client's application extracts the server's public key from the SSL ID. The client's application then generates a unique session key. Session keys are used to encrypt and decrypt all subsequent communication between the client and the server. Using the server's public key, the client's application encrypts the session key and sends a copy of it to the server.
5. Using its private key, the server decrypts the session key. At this point, the server and client both have a copy of the session key. All subsequent communication between the server and client is encrypted with this session key. At the end of the session, the session key is discarded.

Premium SSL IDs

Premium SSL IDs are very similar to SSL IDs. However, Premium SSL IDs offer stronger SSL sessions for export-grade browsers. While SSL IDs offer only 40-bit SSL sessions for export-grade browsers, Premium SSL IDs provide 128-bit SSL sessions. Thus, Premium SSL IDs ensure that all Web site visitors can communicate at the highest possible SSL encryption (128-bits), regardless of their browser type or their physical location.

With Premium SSL IDs, end users do not need to purchase or install any special software. In addition, your organization is not required to obtain special licenses or escrow keys. Premium SSL IDs provide the simplest way to ensure universally strong encryption in your SSL environment.

Certificate Standards

All VeriSign Managed PKI certificates comply with the X.509 international standard, the most widely accepted certificate format.

+ End-user IDs support the S/MIME secure email standard. MIME (Multipurpose Internet Mail Extensions) is the official proposed standard for

Internet electronic mail. S/MIME (Secure/MIME) is a MIME protocol that adds the digital signature and encryption capabilities of the Public Key Cryptography Standards (PKCS). PKCS is a set of standards designed for public-key cryptography. With S/MIME, an email application can support the privacy, identity, nonrepudiation, data integrity, and authentication capabilities of PKCS.

+ SSL IDs are issued as part of a PKCS#7 chain, and may be used to implement Secure Sockets Layers (SSL).
+ IPSec Digital IDs (for IPSec-compliant devices) support Simple Certificate Enrollment Protocol (SCEP).

For more information about certificate technology, visit VeriSign's Web site at: **http://www.verisign.com/support/index.html**.

Issuing Certificates with Managed PKI

With Managed PKI, your organization may elect to use either public or private certificates.

Public Certification Authority

Public certificates are used to secure access to intranets, extranets, and e-commerce applications on a broad scale. Used with the VeriSign Trust Network (VTN), public certificates are interoperable, allowing you to communicate outside of your private domain. Certification Authorities within the VeriSign Trust Network are governed by the VeriSign Certification Practice Statement (CPS). If you elect to use public certificates, you will issue and manage certificates with a Certification Authority in the VeriSign Trust Network.

Chapter 3, "Enrolling For Managed PKI," discusses the benefits of public certification.

Private Certification Authority

In contrast to public certificates, private certificates can only be used within your organization's private domain hierarchy. To issue private certificates within a private domain, your organization must create its own Certification Authority. Since private hierarchies are not part of the VTN, your organization will not be governed by the VeriSign Certification Practice Statement (CPS). Instead, your organization may craft its own set of practices. However, your organization may purchase a license to employ VeriSign's CPS with your private domain.

Chapter 3, "Enrolling For Managed PKI," discusses the benefits of private certification.

CRL Management

A certificate revocation list (CRL) is a list of certificates that have been revoked prior to their expiration dates. Subscribers use CRLs to determine the validity of certificates for people or Web sites with whom they are communicating. VeriSign updates the CRLs daily with standard service, or hourly with Premium Revocation Service.

Generally, a CRL includes:

- The CRL issuer's name
- The date of issue
- The scheduled date of issue for the next CRL
- The serial numbers of the revoked certificates
- The specific times and reasons for suspension and revocation

For customers using public certification, CRLs list all non-expired, revoked certificates for your CA. For private certificates, CRLs contain all non-expired, revoked certificates within your private CA's domain.

To download a CRL, go to the *Certificate Management* page of the VeriSign Control Center, and click the **Download CRL** link. The Control Center can only be accessed with a Managed PKI administrator ID.

Certificate Validation Module (CVM) Kit

To assist customers in working with CRLs, VeriSign provides the Certificate Validation Module (CVM) Kit. This kit includes a Web server plug-in that automatically retrieves CRLs.

The Web server plug-in checks the validity of all certificates presented to the Web server. Thus, subscribers with revoked certificates are unable to access sensitive information. The plug-in acquires CRLs from local files, HTTP servers, and/or LDAP servers. The plug-in caches the CRLs in a local directory on the Web server, and refreshes them when necessary. Before trusting an incoming message, the plug-in always verifies the digital signature of the message. The plug-in is fully configured with a text file, and can be operated in manual or automatic mode.

To download the Certificate Validation Module (CVM) Kit, go to the *Software Download* page of the VeriSign Control Center. Click the **Certificate Validation Module (CVM) Kit** link. A license agreement appears. To accept the license and download the toolkit, click **Accept**. Select the appropriate Web server, and a wizard will guide you through the download and installation process.

For more information about certificate management, see *Managed PKI Administrator's Handbook*.

Managed PKI Directory Structure

This chapter identifies and describes the directory structures included with Managed PKI. Your Managed PKI configuration determines which directories are installed on your system.

This chapter includes the following topics:

- "Adding Directory Structures" on page 43
- "Local Hosting Directory Structure for the <webroot> Directory" on page 44
- "Registration Authority Directory Structure" on page 45

Adding Directory Structures

Once you have acquired and installed your administrator ID, you configure Managed PKI with the Policy Wizard (see *Managed PKI Installation and Configuration*). When you complete your configuration, Managed PKI prompts you to download your policy file. If you have implemented locally-hosted Managed PKI, you then use the Managed PKI Local Hosting CD and policy file to install and configure the necessary directories and files.

Some Managed PKI directories and files, such as the Automated Administration files (see Figure 5-2 on page 45), are automatically installed during the installation of Managed PKI. However, other Managed PKI options, such as Local Hosting, require that you manually create the appropriate directories. Once the requisite directories have been installed, you must configure your Web server to access the appropriate subdirectories of the installation directory: the document root (htmldocs) and program root (cgi-bin).

Note VeriSign recommends that you create an installation directory in the root drive (typically, the C: drive in Windows systems):

VeriSign\MPKI\webroot

Local Hosting Directory Structure for the <webroot> Directory

When you install Local Hosting from the Managed PKI CD, you specify the destination directory (typically VeriSign\MPKI\webroot). Figure 5-1 illustrates the <webroot> directory.

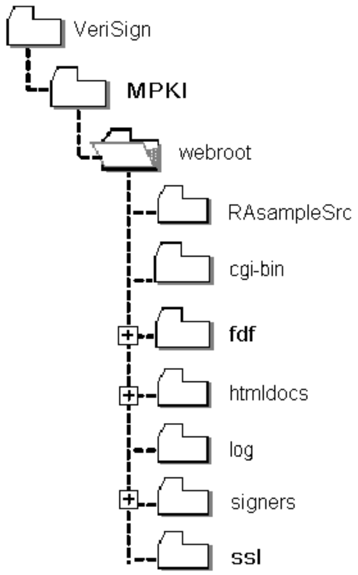

Figure 5-1 Local Hosting directory structure

The Local Hosting <webroot> destination directory includes the following subdirectories:

- AAsampleSrc — Contains sample files
- cgi-bin — The program root containing CGI programs
- fdf — Contains files used by VeriSign CGI programs to validate data entered in enrollment forms
- htmldocs — The document root containing HTML files and graphics
- log — The directory to which various log files will be written
- signers — Contains files specific to Automated Administration
- ssl — Contains the software and certificates used to authenticate/encrypt the connection between the Local Hosting Server host and the RA Server host

Registration Authority Directory Structure

When you install Registration Authority, subdirectories are automatically installed in the Auto Admin directory. Figure 5-2 illustrates the Auto Admin directory.

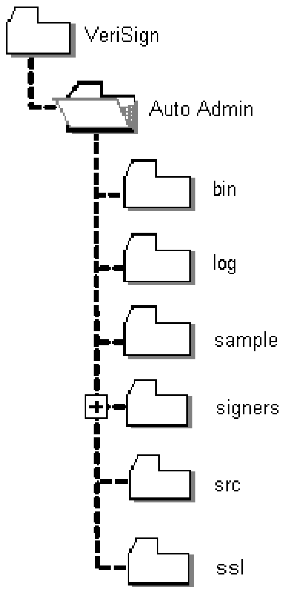

Figure 5-2 Registration Authority directory structure

The Auto Admin directory includes the following subdirectories:

- bin - Contains program files
- log - The directory to which various log files will be written
- sample - Contains sample scripts for testing Registration Authority, such as SQL scripts that you can use to create test tables in ODBC-compatible databases
- signers - Contains library files and utilities
- src - Contains source files
- ssl - Contains the software and certificates used to authenticate/encrypt the connection between the Local Hosting Server host and the RA Server host

Index