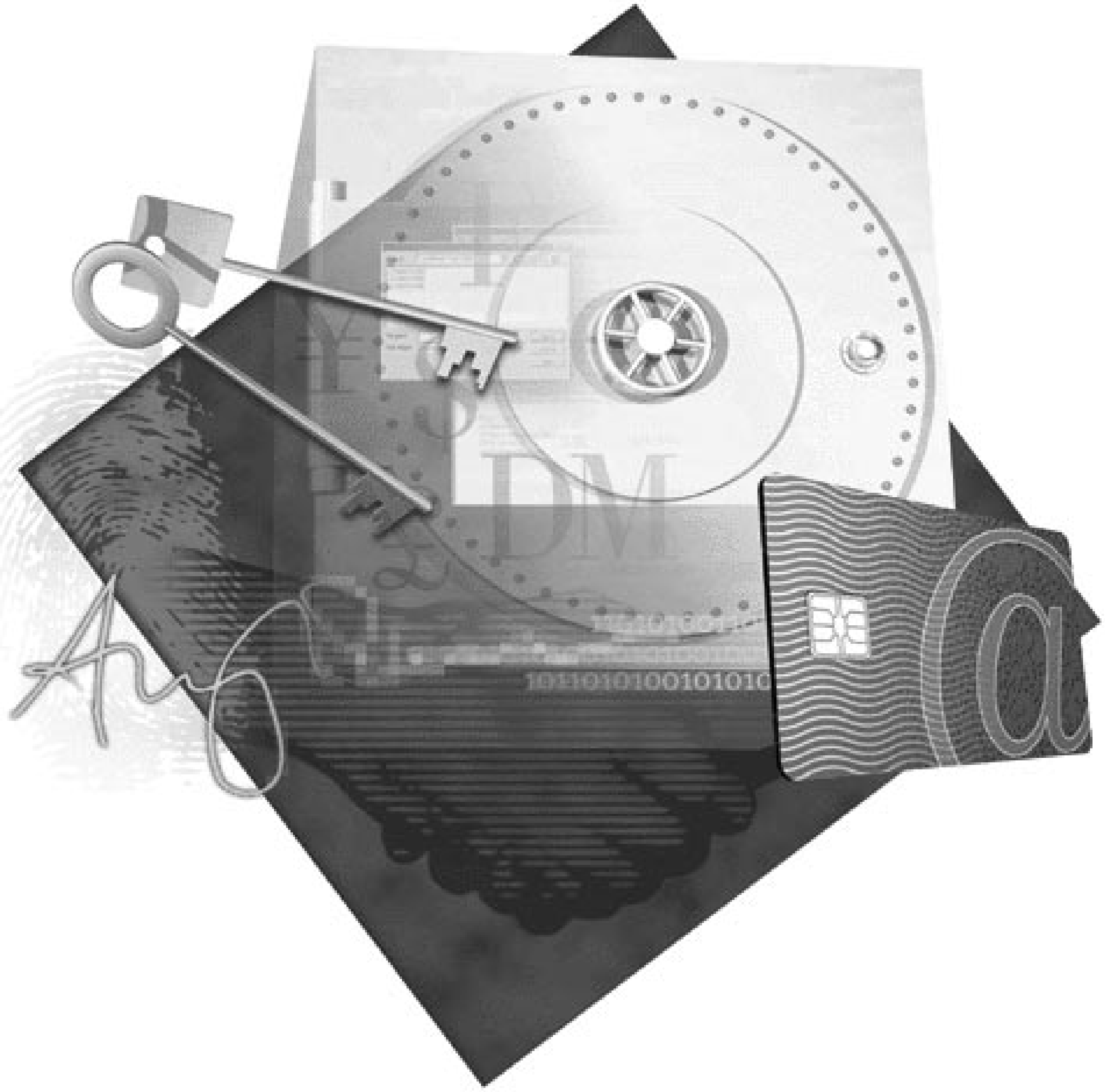
IBM Vault Registry

# General Information Guide

*Version 2 Release 2.2*



GH09-4516-02

IBM Vault Registry

# General Information Guide

*Version 2 Release 2.2*

GH09-4516-02

**Note!**

Before using this information and the product it supports, be sure to read the general information under “Notices” on page vii.

**Third Edition (March 1999)**

This edition applies to Vault Registry, program 5648-B28, version 2 release 2 modification 2, and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# Figures

# Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

The information contained in this document is distributed ″as is.″ The use of this information or the implementation of any of the techniques described herein is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. There is no guarantee provided that this information or these techniques will yield a particular result in your environment. Customers attempting to adapt this information or these techniques into their own environment do so at their sole risk.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Commercial Relations, IBM Corporation, Purchase, NY 10577, U.S.A.

## Trademarks and Service Marks

The following are trademarks of International Business Machines Corporation in the United States and/or other countries:

- IBM
- AIX
- AIX/6000
- DB2
- DB2 Universal Database
- eNetwork
- NetView
- RISC System/6000
- RS/6000
- SecureWay

IBM Vault Registry includes certificate management software licensed originally from Northern Telecom Inc., now Entrust Technologies Inc.

Java and HotJava are trademarks of Sun Microsystems, Inc.

Lotus Domino Go is a trademark of Lotus Development Corporation.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

This program contains security software from RSA Data Security, Inc.

Other company, product, and service names may be trademarks or service marks of others.

# About This Book

This book introduces the IBM® Vault Registry product, an integrated solution for managing the registration and certification of trusted e-business parties. It describes the system and includes scenarios that show how to use vault technology to implement secure, trusted applications in your enterprise.

This book attempts to answer the following questions:

- What is Vault Registry?
- What can it do for your organization?
- How does it work in an actual business situation?

## Audience

This book addresses a varied audience that includes managers, programmers, system administrators, and operators. It can help:

- Marketing managers searching for ways to take advantage of Web-based commerce to help sell their organization's applications securely.
- Security managers seeking the confidence that comes with knowing that their organization's transactions are being processed more securely on the Internet and their intranets. This book can help them understand the Vault Registry technology so they can incorporate it into their organization's security framework.
- Programmers, operators, and administrators looking for a clear understanding of the technical capabilities of a technology that more securely processes their organization's registration transactions on the Internet and their intranets.

This book assumes that the reader has some experience with the World Wide Web and the Internet. It does not assume any previous experience with the Vault Registry solution.

## New in Release 2.2

New features in Vault Registry version 2.2 include:

- Directory-neutral architecture providing greater flexibility with respect to whichever Directory your organization chooses to use.
- Virtual Private Network (VPN) support. With the Vault Registration Application, users can register and obtain credentials for VPN products. This feature includes the ability to obtain Entrust IDs for products enabled through the EntrustIPSec Negotiator Toolkit (software available from Entrust Technologies, Inc.).
- Support for Secure/Multipurpose Internet Mail Extensions (S/MIME) in certificates issued through the Vault Registration Application. This feature enables e-mail sent through S/MIME-capable clients, such as Netscape Communicator (using Messenger) and Microsoft Internet Explorer (using Outlook Express or Outlook 98) to be signed and encrypted.
- Support for backing up and restoring the system repositories in online mode, and for reconciling the system to the best possible state with regard to the Vault Registration Application databases.

- The ability to configure application domains for Master RA users. Using a modified version of the RA Desktop, these users approve and administer certificates for users who enroll as RA administrators and Vault Registry operators. Administrative privileges can now be granted on an application domain-specific basis.
- The ability to configure a unique validator vault per application domain. In prior releases, requests from users who did not possess vault access certificates were processed by a single validator vault in conjunction with the Vault CA. Now multiple validator vaults can be used in conjunction with application-specific CAs, allowing the registration workload to be distributed among multiple processes.

## Organization

This book contains the following chapters:

- "Chapter 1. Introduction to IBM Vault Registry" on page 1 discusses the advantages of using the Vault Registry solution for your Web-based registration and certification. It presents a simplified model of the Vault Registry solution detailing its benefits to your organization.
- "Chapter 2. Vault Registry Technology" on page 9 lists the main components of the Vault Registry solution and presents an in-depth discussion of the technology that forms the foundation of Vault Registry.
- "Chapter 3. Supported Standards" on page 23 lists the security standards that IBM Vault Registry supports or complies with and the different encryption levels used in a Vault Registry system.
- "Chapter 4. System Requirements" on page 25 lists the hardware and software required for your organization to run the Vault Registry system.
- "Chapter 5. Vault Registry Applications and Scenarios" on page 29 presents two business scenarios showing the use of the Vault Registry technology by organizations to control registration and certification for their e-business and other sensitive applications.

This book also contains copyright notices pertaining to this product, a glossary of terms and definitions, and a bibliography.

## Conventions

This book uses the following typographic conventions:

| **Convention** | **Meaning** |
|---|---|
| **bold** | First use of special terms that are relevant to IBM Vault Registry. |
| `monospace` | Paths, syntax, sample code, and window elements (such as menus and buttons selected by the user). |
| **`bold monospace`** | Text the user must type. |
| *italic* | Variable values the user must supply. |
| → | Shows a series of selections from a menu. For example: Select `File` → `Run` means click on `File` and then click on `Run`. |

## Additional Information

The IBM Vault Registry distribution package includes the *IBM Vault Registry General Information Guide* and *IBM Vault Registry Installation and Configuration Guide* in printed form. Those books, and all other Vault Registry publications, are also distributed as Postscript (PS), Portable Document Format (PDF), and HTML files on the *IBM Vault Registry Documentation* CD-ROM. Many of the books have been translated to the languages Vault Registry supports. To learn how to view and print the files, see the *Readme_en* file on the documentation CD-ROM.

The *Readme_en* file also contains information about how to access related publications that may help you administer, use, or develop applications for Vault Registry. For example, you can obtain information about using IBM eNetwork™ Directory API functions, or print books that describe the IBM Vault Certificate Management System in detail.

**Note:** Information in the softcopy books may be more current than the printed manuals. For the latest product information, see the *Readme* file distributed on the *IBM Vault Registry Code* CD-ROM. That *Readme* file contains last-minute additions and changes to the requirements and procedures documented in the books.

The IBM Vault Registry library includes the following books:

- *IBM Vault Registry General Information Guide*

  This book introduces the Vault Registry product, an integrated solution for managing the certification of trusted e-business parties. It describes the system components and includes scenarios that show how to use vault technology for secure, trusted applications in your enterprise.
- *IBM Vault Registry Installation and Configuration Guide*

  This book provides procedures for installing and configuring Vault Registry server components: Vault Controller, Vault Certificate Management System, Vault Registration Application for AIX, and corequisite products.
- *IBM Vault Registry System Operations Guide*

  This book provides information about monitoring and administering a Vault Registry system. It includes information about logging, reporting, and backup and recovery.
- *IBM Vault Registry Messages and Codes*

  This book lists messages that are produced by the Vault Registry product components. The message descriptions explain how to resolve the errors.
- *IBM Vault Controller for AIX Programming Reference*

  This book provides an application developer with a complete reference to the syntax of each Vault Controller application program interface (API) function.
- *IBM Vault Controller for AIX Programming Guide*

  This book shows an application developer how to write a vault-based application that uses the API functions documented in the *IBM Vault Controller for AIX Programming Reference*.
- *IBM Vault Agent User Guide and Reference*

  This book provides procedures for installing, configuring, and developing applications for the Vault Agent client component. The book includes a complete reference to the syntax of each API function provided for the Vault Agent.
- *IBM Vault Certificate Validator User Guide and Reference*

This book provides procedures for installing and developing applications for the Vault Certificate Validator client component. The book includes a complete reference to the syntax of each API function provided for the Vault Certificate Validator.

- *IBM Vault Registration Application for AIX Customization Guide*

  This book provides an application developer with information about how to customize the Vault Registration Application according to the needs and preferences of your organization's secure e-business goals.

- *IBM Vault Registry Registration Authority User Guide*

  This book shows a registration authority (RA) and Master RA user how to use the RA Desktop to administer requests for certificates.

# Chapter 1. Introduction to IBM Vault Registry

This chapter provides an overview of some of the ways organizations have addressed security issues for their software applications. It describes both the methodology traditionally used to deny access to their software applications by intruders and the inherent limitations of that methodology. The chapter also describes a newer approach, referred to as **public key infrastructure (PKI)** technology, that many organizations are using to secure their Internet transactions. Finally, the chapter presents the IBM® Vault Registry solution, which offers a customizable registration application that uses a PKI as the basis for the implementation of an innovative vault technology. This application is called the IBM **Vault Registration Application** for AIX®.

## Internet Security Requirements

A discussion of Internet security requirements is a necessary introduction to a description of Internet security solutions. The explosive growth of the Web has led to a significant increase in the number of organizations using the Internet for conducting e-business. Unfortunately, this growth has also increased the potential for crime. To reap the benefits of the global reach of the Web, all organizations must establish security policies that protect them from the security risks intrinsic to this hostile environment.

Organizations can protect their business applications and assets in e-business by developing security policies that dictate the types of networked transactions that are used. These networked transactions should provide:

- Strong mutual **authentication**

  Parties in a transaction are confirmed to be who they claim to be.
- **Confidentiality**

  Sensitive data in a transaction is kept secret and disclosed only to authorized parties.
- **Integrity**

  Information in a transaction is protected against tampering and corruption.
- **Non-repudiation**

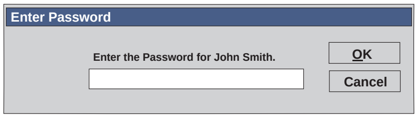
  Recipients are protected against senders denying that they originated a message.
- **Access control**

  Access to secured data and information is determined by your organization’s policies and protocols.
- **Audit trail**

  A history of major events (for example, certificate issuance) and policy security violations are archived.

## Before Vault Registry: Password-Based Security

Traditionally, organizations have used password-based security systems — user identifications (user IDs) and passwords — to register their users and control their users’ access to the organizations’ software applications.



Enter the Password for John Smith.

In the traditional password-based security methodology, a user ID and password establish a user's identity for accessing an organization's secured information. The password is the key that authenticates the user ID. The user ID-password pair becomes a key that unlocks the door that protects an organization's information. However, this password-based system does not provide the security that an organization needs for today's e-business. Passwords have the following characteristics:

- They can be compromised by onlookers during logon.
- They can be easily intercepted on the Internet if the transaction is not safeguarded with a secure Web protocol such as **Secure Sockets Layer (SSL)**.
- They authenticate a user to a host, but not a host to a user.
- They can be discovered using automated trial and error techniques.
- They do not protect transmitted information.
- They can be repudiated.

When your organization conducts e-business, password-based security neither protects information nor ensures that access is limited to authorized entities and software applications. It allows others to impersonate you once they know your password. Passwords alone are insufficient for secure e-business.

## A Newer Approach: Public Key Cryptography

**Digital keys** are replacing user ID-password pairs in e-business. Public key cryptography uses mathematically related **public-private key pairs**. Only the private key can decrypt the information the public key has encrypted. The **public key** can be made available to anyone. The **private key** is kept secret by its holder.

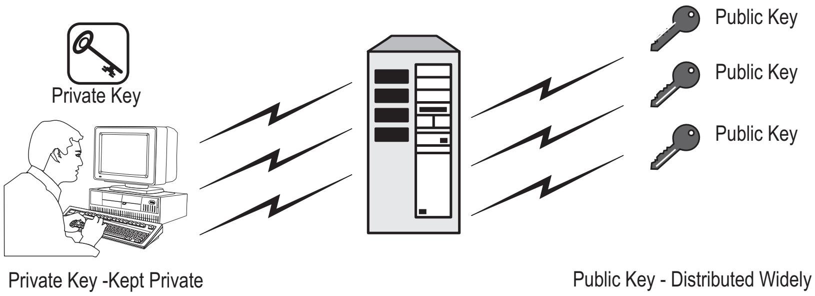


*Figure 1. Public-Private Key Pairs*

Just as digital keys are replacing user ID-password pairs in e-business, **digital signatures** are replacing physical signatures. A digital signature is a coded message affixed to a document or data that helps guarantee the identity of the sender, thereby providing a greater level of security than a physical signature. A digital signature identifies the sender because only the sender's private key can create the signature. It also helps ensure that the content of the signed message cannot be altered without the recipient being able to discover that it has been altered.

**Digital certificates (certificates)** are also replacing their physical counterpart — hardcopy credentials — in e-business. Issued by a **certificate authority (CA)**, a certificate vouches for (or certifies) the public key of an individual, software application, organization, or business. It performs a role similar to that of a driver's license or medical diploma — it certifies that the bearer of the corresponding private key is authorized (by an organization) to conduct certain activities.

The life cycle of digital certificates is similar to that of physical certificates. For example, digital certificates can be issued and revoked. When a certificate is issued (after the user is authorized), the certificate holder is given the right to use the certificate for a specified amount of time. When a certificate is revoked, the certificate holder permanently loses the right to use the certificate. Certificates can also be deferred, or they can expire. When they are deferred, they are kept in a pending state until additional information is obtained.

Secure applications must check the validity period of a certificate to determine whether the certificate is valid. They must determine whether a certificate has expired or been revoked. They must also determine whether the start of the validity period has passed.

## The Vault Registry Solution

IBM Vault Registry is an integrated registration and certification solution for enabling trusted e-business applications. It is for organizations moving e-business applications to the Internet to establish security and trust.

While digital certificates are evolving as an accepted means for authentication and access control over untrusted networks, the certificates are only as valuable as the degree of trust and security involved in registering and certifying the participants. Vault Registry enables trusted e-business applications on the Internet by providing a robust, integrated, security-rich solution for managing the **registration** and issuance of digital certificates (**certification**) to trusted entities.

The Vault Registry technology uses the concept of an **electronic vault (vault)** to provide enhanced security throughout the registration process. It provides the IBM Vault Registration Application, to enable those wanting to use trusted **e-commerce** offerings (such as banking, insurance, and health care) to register themselves. The applicants supply the information to be used to prove their right to participate in desired business transactions.

With Vault Registry, your software applications can reside either on a standard Web server or in the enhanced Vault Registry Web server environment. Your end users can access either server from a standard Web browser using the SSL protocol. SSL is a standard used by Web browsers and servers for secure communications.

In summary, the Vault Registry solution addresses the challenges of secure and trusted computing on the Internet. It is crafted from security technologies that are solidly based on industry standards, and provides certificates and cryptographic keys managed by secure databases and secure servers.

### Vault Registry Registration and Certification Process

Using the Vault Registry solution, an authorized registrar, or **registration authority** (**RA**) administrator at your organization performs the following tasks:

- Reviews the information that applicants provide

- Performs any additional verification that your organization requires
- Determines whether applicants should be authorized to access secure applications or services such as financial accounts, stock quotes, or stock trading
- Approves or rejects the applicant's request

Once approved, applicants receive credentials that attest to the validity of the keys they use for accessing your organization's applications. This process is known as registration and certification.

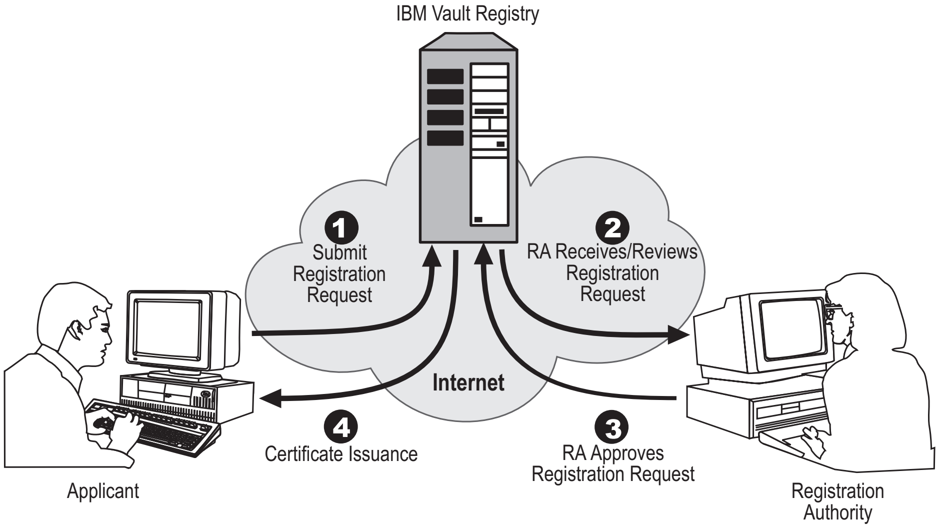

IBM Vault Registry
1
Submit Registration Request
2
RA Receives/Reviews Registration Request
Internet
4
Certificate Issuance
3
RA Approves Registration Request
Applicant
Registration Authority

*Figure 2. Vault Registry Registration and Certification Process*

Figure 2 illustrates a typical Vault Registry registration process which consists of the following four steps:

1. An applicant submits a registration request.

   Using a Web browser that supports browser certificates and a Vault Registration Application customized for your organization, an applicant completes and submits a registration form. At this time, the Web browser generates a public-private key pair. The contents of the form and the public key are then transmitted by way of the SSL protocol to the Vault Registry server for processing by your organization's RA administrator.
2. An RA administrator receives and reviews the registration request.

   Your RA administrator uses a Web browser that supports client certificates to view applicants' pending registration requests. Only the RA administrator and the applicant are able to view these requests. This helps to ensure that sensitive information provided by the applicant is kept private and secure throughout the registration process.

   The RA administrator reviews each registration request. As part of the review, the RA administrator may need to perform additional verification of the applicant's request as determined by your organization's policies. This verification can be performed in many ways. For example, the RA administrator can contact the applicant to make sure that the applicant (and not someone else) submitted a registration request. The RA administrator can also validate the request by viewing information in the registration form known only to the applicant and the RA administrator.

The RA functions can also be automated, running checks against backend systems and databases. Whatever the method, your organization has total control of the registration approval process.

**Note:** Your organization may, if desired, assign RA administration responsibilities to more than one person.

3. An RA administrator approves the registration request.

   Using your organization's Vault Registration Application, your RA administrator indicates whether an applicant's registration request should be approved or rejected.
4. Either a certificate or a credential for accessing VPN products is issued to the applicant.

**Note:** Throughout the registration process, the information provided by the applicant is stored in an RA database and transmitted between processes in encrypted form. In addition, the RA administrator provides ongoing administration of all certificates throughout their life cycle.

## Why Use Vault Registry?

IBM Vault Registry leverages over 30 years of industry-leading research and technology in providing security for digital assets. Vault Registry provides:

- Innovative **vault** software that protects data and applications from disclosure to unauthorized users.
- A secure registration process that helps ensure that digital certificates are worthy of trust.
- A flexible approach that enables integration with existing applications and customization for unique business policies.
- A scalable base that can be extended to support registration and certification processes across organizational boundaries and under consolidated system and operations management.

### Enhanced Trust Model Using Vault Technology

Vault Registry extends traditional Web processing by running registration applications in a vault. A vault is a secure storage area on a server that runs programs and services on behalf of an authorized user. IBM has pioneered vault software that uses encryption to isolate data and applications by responsibilities and roles — including protection from unauthorized system administrators. A vault can be compared to a safe deposit box at a bank that protects an individual's valuable assets, even from bank employees. For a detailed description of a vault see "Chapter 2. Vault Registry Technology."

### A Secure Registration Process

Through the Vault Registration Application, Vault Registry technology provides an **end-to-end security** solution by enforcing your organization's security policies throughout the life cycle of the application:

- SSL is used for protecting information transmitted between the browser and the server, and for authenticating the users of the browser and the server.
- Information stored in the Vault Registry product is protected by keeping sensitive information encrypted and signed in vaults accessible only to the owners of the vaults.
- Information transmitted between vaults is protected by encryption and signing.

- Information stored in the Vault Registry databases is also encrypted.

The Vault Registration Application helps ensure that online business can be conducted with even more confidence than physical-world business by greatly enhancing the security and integrity of the registration business process that identifies and authorizes parties in a transaction.

## Customizable Registration Process

With the Vault Registration Application, Vault Registry offers the flexibility to customize the registration process for unique business policies. It is designed to integrate with backend systems to protect and leverage investments.

Your organization can customize all steps in the registration approval process so that its security policy is implemented. Successive steps in the registration process can occur minutes, hours or days apart allowing a registration process of several disjointed steps to be performed as securely as a single secure transaction. Your organization can do the following:

- It can decide how applicants are to submit registration requests. For example, you may elect to have your users complete a specific form.
- It can designate RA administrators for reviewing registration requests.
- It can organize the RA administrators into separate, isolated domains, if necessary.
- It can set the standards for your RA administrators' decisions. Do they need to check an individual's credentials? Do they need to require that individuals physically appear in their presence to present their credentials for review?
- It can identify the level of detailed information to request from applicants.
- It can determine whether RA activity will be handled by humans, automated processes, or a combination of both.

## Robust System Operations and Management

The integration of vault software with a PKI enables the implementation of multiple registration and certificate authorities under consolidated systems and operations management.

**Online Recovery and Repository Reconciliation:** In addition to its offline backup and restore capabilities, Vault Registry provides independent online backup and restore capabilities for each of the Vault Registry repositories. The Vault Registry system also provides a reconciliation tool for the Vault Registration Application. This utility performs integrity checking to provide, in most cases, data reconciliation across the entire system, thereby restoring it to a best-possible state of recovery. This tool is accessible only through the operator vaults within the **Operations Center**.

**Operations Center:** The Vault Registration Application supports a set of functions, via an interface referred to as the Operations Center, that are intended for operations support. Operators are given specially authorized operator vaults through which they can access the Operations Center functions. Operations Center functions include the capability to generate Vault Registration Application database reports, perform database reconciliation, and process vault enrollment requests for users who want to enroll as RA administrators or operators.

In general, these operations functions provide read-only access to aggregate and non-confidential information. Because the Vault Registration Application supports an open interface for incorporating new functions using simple HTML coding and Vault Registration Application configuration, your organization can add or modify reports and functions as needed.

**Reporting:** In addition to the vault-based reporting capability that allows an operator to run customized database and other system reports displayed in HTML, predefined reports are available on the number of certificates issued, revoked, and renewed per CA over its lifetime.

**Monitoring and System Management:** Vault Registry monitors critical system components and attempts to automatically restart all failed components. In the event of system failures or other exceptional error conditions, it can deliver **Simple Network Management Protocol** (SNMP) traps to any system management console that supports SNMP. These SNMP traps are created from system or application events that include:

- Component failures
- Components failing to respond
- Inability to complete tasks
- Other error and informational messages

**Logging:** To enhance recoverability and non-repudiability of transactions, Vault Registry maintains auditable logs of all registration and certificate processing transactions.

# Chapter 2. Vault Registry Technology

This chapter provides an overview of Vault Registry technology. It describes the Vault Registry components briefly and makes a more detailed presentation of the major aspects of Vault Registry server technology. Finally, use of a remote Vault Agent application to interact with the Vault Controller functionality is described.

## Vault Registry Components

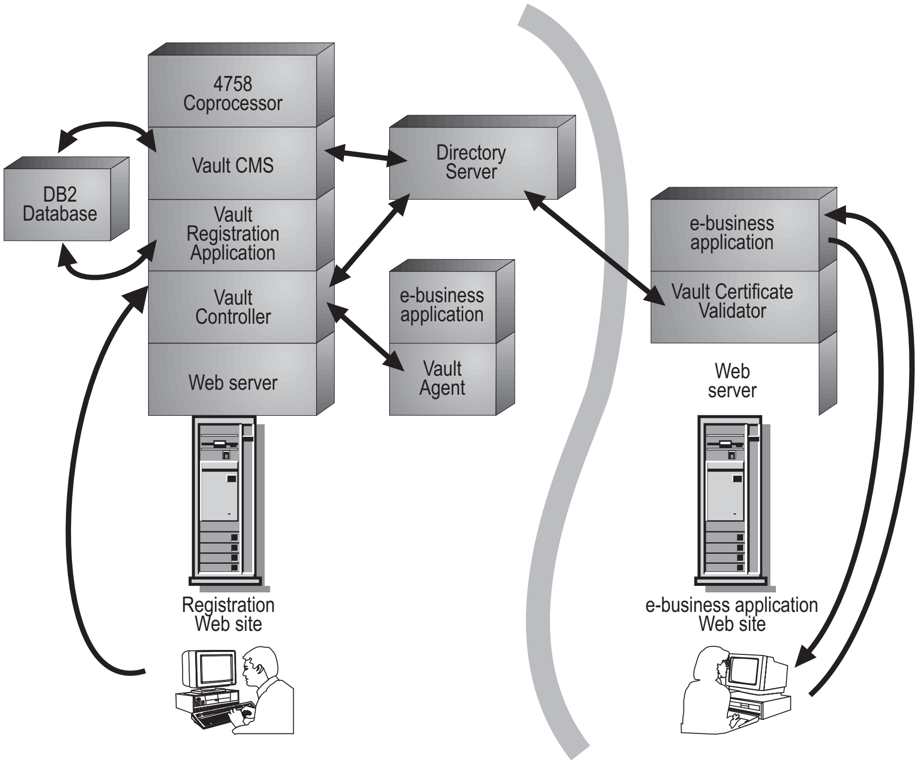


*Figure 3. Vault Registry Components*

The Vault Registry product is composed of the following major components:

- **Vault Controller**

  The IBM Vault Controller is an enhanced secure Web server that provides vaults for users, RAs, operators, and certificate authorities. A vault provides a secure environment within the Vault Registry server for executing programs and applications on behalf of a user. Vaults, and their contents, are accessible from SSL-enabled Web browsers (**clients**) that contain the corresponding **vault access certificate**s.

  Information stored in vaults is protected against the following:

  – Disclosure to unauthorized persons (such as system administrators and other vault owners) by encryption

  – Tampering by digital signature

  – Untrusted communications with unknown parties by authentication using digital certificates

Information can also be transmitted securely to other vaults using encryption, digital signatures, and certificates.

All vaults managed by a single instance of the Vault Controller use a single instance of a vault certificate management system. This instance, called the Vault CA, issues and manages the vaults' encryption, signing, and vault access certificates.

For a detailed discussion of Vault Controller technology, refer to "Vault Controller" on page 11.

- **Vault Certificate Management System** (**Vault CMS**)

  The IBM Vault CMS enables a CA to issue, renew, and revoke **X.509v3** certificates as well as credentials to access Entrust-ready VPN products that can be used with software from Entrust Technologies Inc. It also allows the CA to update and publish certificates, **certificate revocation list**s (**CRL**s), and organization policy information in a Directory. It includes components that are based on software from Entrust. For a detailed discussion of CAs and certificates, refer to "Certificate Authority and Certificates" on page 15.

- Vault Registration Application

  The IBM Vault Registration Application for AIX is a customizable registration application that runs on the Vault Controller. It has been built to fully utilize the Vault Controller environment. It enables organizations to register users for their services and administer the issued credentials (such as certificates) over their life cycle. It has been written to be very flexible, allowing an organization to easily make changes to meet its needs. Refer to the *Vault Registration Application for AIX Customization Guide* for detailed information on modifying this application for your organization.

  Integrated into the Vault Registration Application is a Java applet called the **Registration Authority (RA) Desktop**. The RA Desktop has been built to enable your RA administrators to do the following:

  – Receive applicants' requests for credentials (such as certificates) to access your organizations' services.

  – Approve and reject credential requests.

  – Revoke credentials.

  – Set the renewal status of credentials.

  – View registration requests by category.

  A modified version of the RA Desktop, the Master RA User Desktop, enables a Master RA user to process registration requests from RA administrators and operators. Refer to the *Registration Authority User Guide* for detailed information on using the RA Desktop at your organization.

- **Lotus Domino Go Webserver**

  The Domino Go Webserver is the underlying Web server platform for the Vault Controller and the Vault Registration Application. It is a prerequisite for the installation of the Vault Registry product.

- **Directory Server**

  The Vault Registry product is Directory technology neutral. The PKI data that Vault Registry stores in the Directory includes X.509v3 certificates, CRLs, CA policies, and other information about registered users and servers. An authorized user or software application can find a public key certificate for a particular person or server by searching the Directory for that person's or server's unique **distinguished name** (**DN**) or other relevant information.

Through the use of the Directory, the Vault Registry server provides the scalability needed to support large numbers of users. Your organization can store public key certificates as well as other information needed to enable secure communications in the Directory.

A Directory that meets the standards described in "Chapter 4. System Requirements" on page 25 is a prerequisite for the installation of the Vault Registry product. For more information, refer to "Directory Server" on page 19.

- **IBM DB2® Universal Database (UDB)**

  The Vault Registration Application and Vault CMS use the DB2 UDB to store data and maintain transaction logs for auditing, reporting, and recovery purposes. It is a prerequisite for the installation of the Vault Registry product.

- **Vault Agent**

  The IBM Vault Agent is an optional client program that is available separately from the Vault Registration Application. Using PKI technology, it enables your organization to securely encrypt, exchange, and store data in remote vaults. The Vault Agent library incorporates a subset of the Vault Controller's application programming interface (API) – functions that enable it to exchange secure messages with vaults under the control of the Vault Controller or another vault. It can be run on a Windows NT as well as an AIX platform.

  For more information about the Vault Agent, refer to "Vault Agent" on page 20 and for a detailed discussion, see *Vault Agent User Guide and Reference*.

- **Vault Certificate Validator**

  The IBM Vault Certificate Validator provides a means for client or server programs to validate a certificate at the time credentials are presented for initiation of a business transaction. This is an optional client program that is available separately from the Vault Registration Application. It can be run on a Windows NT as well as an AIX platform. For more information on the Vault Certificate Validator, refer to the *Vault Certificate Validator User Guide and Reference*.

- **4758 Coprocessor**

  The IBM 4758 PCI Cryptographic Coprocessor is the Vault Registry hardware solution. It protects and securely backs up the CA signing key, and minimizes the risks associated with administrator misuse of your system. It is an optional component of the Vault Registry product. For more information, refer to "Hardware Protection of CA Keys" on page 18.

## Vault Controller

The practical application of extensive server knowledge has allowed IBM to develop vault technology. In this technology, a specialized vault server — the Vault Controller — integrates a variety of standard but critical PKI components to create the foundation of the Vault Registry solution.

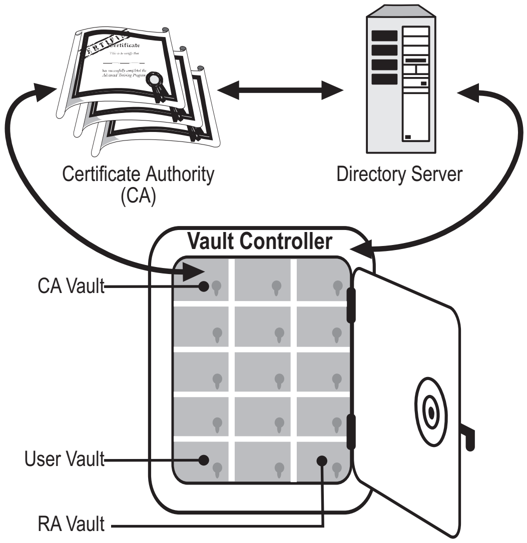


*Figure 4. Vault Controller Technology Components*

## Vault Controller Components

The Vault Controller is the platform on which the certificate registration and administrative programs of an organization run. It consists of the vault process supervisor and the vault process, and is tightly coupled with the underlying Web server, the Domino Go Webserver.

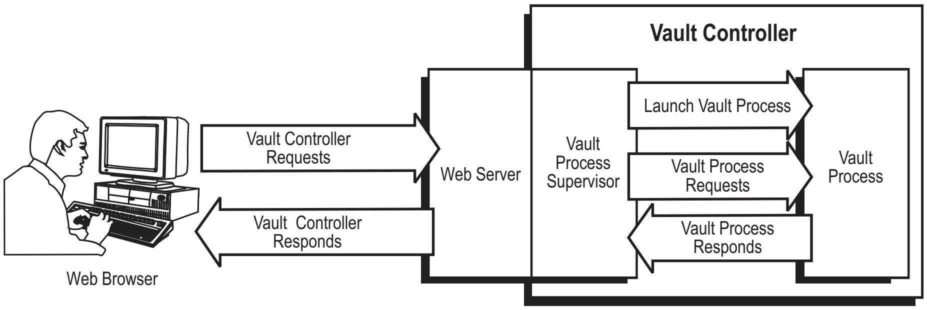


*Figure 5. Vault Controller Components*

- The **vault process supervisor** runs on the Vault Controller and manages all vault processes, the processes that run in vaults. The vault process supervisor does the following:
  - It maps users to their vaults.
  - It launches vault processes as needed.
  - It communicates information posted by a Web browser to a vault process.
  - It forwards vault process responses to the Web browser.
- A **vault process** is a program running in a vault in the Vault Controller. A vault process for an authorized user of one of your organization’s software applications runs on behalf of the user in the vault that belongs to that user. Likewise, a vault process for your organization’s RAs runs on behalf of those RAs in the vaults that belong to them. A vault process also communicates with the CA.

- The Domino Go Webserver is a secure, scalable, high-performance, transaction-ready Web server that does the following:
  - It allows a Web browser to interface with Vault Registry.
  - It allows a Web browser to communicate securely with Vault Registry software via the standard secure Web protocol, SSL.
  - It authenticates a user's digital certificate and key.

## Vaults

The Vault Controller's main function is to host vaults.

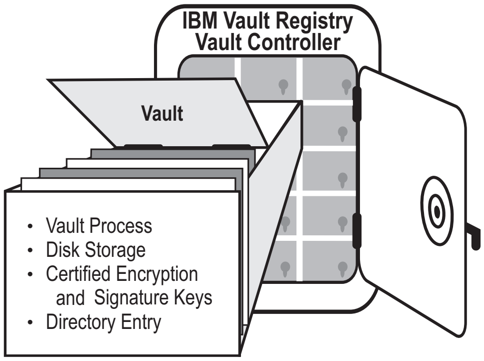


*Figure 6. A Vault*

A vault provides a secure environment within Vault Registry for executing programs on behalf of a user. Each vault consists of the following:

- A vault process

  A vault process runs in the Vault Controller on behalf of a vault owner. Each vault process runs under a unique UNIX user ID. The vault process can be started only by the vault process supervisor and only after a user presents the vault access certificate associated with that vault.

- Disk storage

  Disk storage is owned by the same UNIX user ID that owns the vault process. Using the UNIX file permission scheme, only the user and system administrator have permission to access this disk storage. However, because user vaults are encrypted, the information within them is kept private from the system administrator.

- Certified encryption and signature keys

  Each vault process has two certified public key pairs. One key pair provides encryption and decryption. The other provides digital signing and signature verification.

  Routines for encryption and decryption, digital signing, and signature verification are accessible to processes running in vaults. Vault processes use the **Secure Depositor library** to encrypt and sign data for secure interprocess communications with other vault processes. Vault processes also use the library to decrypt data and verify signatures for data received from other vault processes.

- A Directory entry

A Directory entry stores the vault's public key certificate and additional information. Other vault users use the public key in the certificate to encrypt data for a vault owner so only that vault owner can access it.

## Types of Vaults

Vaults serve multiple purposes in the Vault Registry product. Currently, there are three types:

- A **user vault** is the typical vault designed for use in Vault Registry. A user (for example, a registration applicant, an RA, or an operator) accesses it through a Web browser using a vault access certificate. The vault access certificate is issued during the registration process.
- A **validator vault** is a community vault that is automatically created when Vault Registry is installed. It handles users who do not yet have a vault access certificate. A validator vault can be created for each registration application. A single validator vault process executes in the validator vault to process initial registration requests according to your organization's security policies (for example, pass a credit check or provide minimum personal information).
- A **CA vault** is a vault that is automatically created at installation time. Its sole purpose is to interact with a CA. There is one CA vault per CA. A CA Agent is launched in the CA vault at system start-up. The CA Agent is a customized vault process that accepts RA requests for certificate management services and interacts with the CA to carry them out.

## Vault Controller Features

Within this framework, the Vault Controller provides the following additional features:

- Secure end-to-end communication

  With the use of browser-client authentication and the SSL protocol, the browser request is encrypted and sent to the Vault Controller along with a vault access certificate. The vault process supervisor validates the vault access certificate. Next, it maps the request into the corresponding vault. Finally, it creates a vault process with a corresponding user ID and password by using information from the certificate.
- Reentrant and persistent vault processes

  The vault process supervisor maintains a state table for determining whether a vault process is already running on behalf of a user. If a vault process is already running, the supervisor will attach the user to the existing vault process. The vault process shuts down after a predetermined period of inactivity.
- Multithreaded and stateful vault processes

  Each vault process is multithreaded and able to handle multiple simultaneous requests from the user (who could be running multiple browser instances). Additionally, each thread has its own local storage area allowing it to maintain state across multiple browser-server interactions.
- Inter-vault communications

  Entries in the Directory and the certificates in the vault enable users to encrypt and sign data (through the Secure Depositor library) for any other user on the system that has a vault. This information is safely encrypted with the public key of the recipient.
- Communications with a remote application

The **Secure Depositor daemon** handles communications with a remote application. The remote application sends messages to the Vault Controller through a Vault Agent. The Secure Depositor daemon receives these messages and deposits them into the vault corresponding to the Vault Agent. The daemon runs separately from the Vault Agent or vault processes and can service multiple vaults simultaneously.

# Certificate Authority and Certificates

This section discusses what a certificate authority (CA) is and what it does. It then provides a detailed description of certificates.

## The CA

The CA is a major component of the Vault Registry product that creates and manages certificates for specific trust domains. Each trust domain defines a set of end user entities whose certificates the same CA has certified. Users possessing certificates signed by a CA can trust the identity of another user bearing a certificate signed by the same CA.

But what happens when a user possessing a certificate signed by a CA is asked to trust the identity of a user bearing a certificate signed by a different CA? In this situation, the users and CAs need **cross-certification**. Cross-certification is a **trust model** in which CAs that have established common points of trust sign each other’s certificates.

In Vault Registry, the CA does the following:

- It enforces an organization’s security policies (for example, certificate validity period, key revocation policy).
- It creates and signs public key certificates (X509v3 certificates).
- It issues credentials needed to access Entrust-ready VPN products.
- It publishes certificates and CRLs in the Directory.
- It maintains lists of cross-certified CAs.
- It revokes certificates when requested by authorized RAs.
- It maintains auditable logs of key events.
- It generates the public-private key pairs used in the vaults.
- It manages a secure database allowing for recovery of encryption key pairs.

## CA and Certificate Types

This section summarizes the different types of CAs that Vault CMS supports.

### Vault CA

There is one Vault CA per Vault Controller. This CA issues and manages the encryption keys, verification keys, and certificates generated for each vault. These **internal vault certificates** and their corresponding public keys are stored in profiles that are protected by passwords unknown to any user or administrator.

The Vault CA also issues and manages **vault access certificates**. These certificates and their key pairs are stored in a protected area. They might be stored by the Web browser, in a smart card, or, with Vault Agent applications, in a profile on the

Vault Agent machine. Vault access certificates are used to authenticate users; they permit vault access when a registered entity establishes a secure connection with a vault.

### Organization CA

An Organization CA issues and manages **organization certificates** for Web servers and browsers. Requests for organization certificates are approved or rejected by your organization's RA in accordance with the security policies encoded in your custom implementations of the Vault Registration Application. For example, you can use an organization certificate to certify the identity and authority levels of your employees and customers. You can then use certificates to control access to different computer systems and services, and bypass the need to maintain and distribute access control lists and password files.

Organization certificates can be used to authenticate client access to a Web server that uses the SSLv3 protocol. It allows the certificate owner to be authenticated either by the Web server, if your application is accessed through the server, or by the Vault Controller, if your application also enrolls users for vaults. Depending on the policy exits you write for your applications, organization certificates can also include Secure/Multipurpose Internet Mail Extensions (S/MIME). This feature enables e-mail sent through the Internet to be signed and encrypted.

An Organization CA can also issue **application certificates**. These certificates fall into the following categories:

- Those that do not use the Vault Registration Application, such as custom applications you develop using the Vault Controller and Vault Agent APIs.
- Those that support the Virtual Private Network (VPN) feature of IBM Vault Registry. If your enterprise purchased this feature, users can use the Vault Registration Application to obtain credentials for VPN products. This includes the ability to obtain **Entrust IDs** that enable access to products developed with the EntrustIPSec Negotiator Toolkit.
- Those that may use the Vault Registration Application, but are not intended for use on Web servers or browsers.

Your license agreement with IBM determines the number of Organization CAs that you may configure. To comply with the agreement, you must keep track of the certificates issued by each CA. Different price options apply to different types of organization and application certificates. See the *IBM Vault Registry System Operations Guide* for information about using the Certificate Accounting Tool to track this information.

## X.509v3 Certificate Format

The format of an X.509v3 certificate, which all Vault Registry applications support, is a standard supported by most cryptographic protocols, including SSL. It contains the following fields:

**Version**

The version of the certificate, such as X.509v2 or X.509v3.

**Serial Number**

A unique identifier assigned to the certificate when it was issued by the CA.

**Signature Algorithm Identifier**
An identifier for the digital signature algorithm used by the CA to sign the certificate.

**Issuer** The Directory's distinguished name (DN) of the issuing CA.

**Validity Period**
The time period when the certificate is valid (the date and time the certificate becomes valid and the date and time the certificate's validity expires).

**Subject**
The Directory's distinguished name (DN) of the holder of the private key for which the corresponding public key is being certified.

**Subject Public Key Information**
The value of the subject's public key along with an identifier for the algorithm the public key uses to encrypt information.

**Issuer Unique Identifier**
An optional bit string that validates the CA's name in the event that the same name is assigned to a different entity over time.

**Subject Unique Identifier**
An optional bit string that validates the subject's name in the event that the same name is assigned to a different entity over time.

**CA Digital Signature**
The issuing certificate authority's digital signature.

**Extensions**
Optional fields that store additional information that enables applications to further attest the validity of a certificate.

For complete information about the certificate extensions available to Vault Registry applications, see “Certificate Extensions”. For information about how the Vault Registration Application uses and modifies these extensions, see the *IBM Vault Registration Application for AIX Customization Guide*.

## Certificate Extensions

Extensions in an X.509v3 certificate provide a means for applications to further attest the validity of a certificate. IBM Vault Registry supports many industry-standard extensions. For interoperability, all extensions have the following format:

- A **Type**, which identifies the purpose of the extension field.

  Like encryption and signing algorithms, the extension type must be registered by assigning an object identifier to it. The type also defines the data type (such as text string, integer, or date) of the data in the Value field.
- A **Criticality Indicator**.

  A non-critical extension is one that can be ignored if the application does not recognize the extension type. A critical extension is one that must be recognized and validated by the application before the certificate can be accepted and before any associated function can be implemented.
- A **Value**, which contains the extension data.

The following table summarizes the certificate extensions that Vault Registry applications support. All of the extensions can be modified.

| Type | Criticality | Value |
|---|---|---|
| CertificatePolicies | Non-critical * | Modified as a sequence of Policy IDs (which are Object IDs) only, without qualifiers |
| KeyUsage | Set by the application | Server certificate issuance |
| PrivateKeyUsagePeriod | Non-critical | A routine that sets a range of times into this extension. It is always non-critical. |
| SubjectAltName | Non-critical * | See the following SubjectAltName extension options table for a list of the variants allowed. Note: The S/MIME specification requires that a certificate DN or its SubjectAltName extension contain an e-mail address. |
| * Vault Registry technology requires that this extension be non-critical. | | |

The following table summarizes the `SubjectAltName` certificate extension options. Vault Registry applications currently support those marked "Y" in the `supported?` column.

| Tag # | Option | Supported? | Value |
|---|---|---|---|
| 0 | OtherName | N | An instance of the type identifier information object class as defined in Annex A of ITU-T Recommendation X.681 (ISO standard 8824-2). |
| 1 | rfc822Name | Y | Internet e-mail address |
| 2 | dnsName | Y | Internet host or node name |
| 3 | x400Address | N | X.400 e-mail address in ASN.1 |
| 4 | DirectoryName | N | Directory's DN in ASN.1 |
| 5 | EDIPartyName | N | A name of a term agreed between communicating EDI partners. A component identifies an authority that assigns unique name values in the partyName component. |
| 6 | uniformResourceIdentifier | Y | URL ID |
| 7 | IPAddress | Y | Binary IP address |
| 8 | Registered ID | Y | Object ID |

## Hardware Protection of CA Keys

When a CA uses a signing key to create a certificate, the CA is certifying that the holder of the certificate is authorized to perform specified activities. If an unauthorized user obtains the CA's signing key, that user can create certificates for other unauthorized users enabling them to initiate transactions or gain access to information and resources. To minimize these risks, it is imperative that the CA signing key be protected.

Software-only solutions can protect signing keys using encryption. That is, the software can include algorithms that apply security code to signing keys. However, the signing key must be easily accessible to generate the signature for all software sign operations. This requirement exposes the signing key to capture by malicious individuals.

### Protection of CA Keys in Vault Registry

Because unauthorized disclosure of a CA signing key can lead to significant loss, the Vault Registry product can use special hardware to protect these keys. This hardware minimizes the risks associated with misuse of the system. It should be purchased at the same time that Vault Registry is purchased.

### Integration with Vault Registry CA Component

The Vault Registry CA component works with the IBM 4758 PCI Cryptographic Coprocessor, a member of the IBM SecureWay™ product family. The IBM 4758 helps to ensure the privacy and integrity of your organization's signature key. It uses the IBM Common Cryptographic Architecture (CCA) API to provide a comprehensive set of cryptographic services including DES and RSA encryption.

DES and RSA are the most widely used algorithms in commercial cryptographic systems. However, because they are so strong, the key management methodology that your organization uses becomes the more vulnerable portion of your system. When a key is compromised, the data encrypted with that key may be completely exposed. The IBM 4758 helps extend comprehensive protection to those keys by including:

- Triple-encryption of keys using a special key stored within the dedicated hardware
- Protection of end-to-end data communications
- Definition of user access levels, using a role-based access-control system, for consistent use throughout an organization
- Use of a hardware-based random-number generator to help ensure the creation of unpredictable keys

# Directory Server

Vault Registry uses the Directory for the management, storage, retrieval, and distribution of the following types of data or objects:

- X.509v3 certificates
- CRLs
- Cross-certificates
- Customer-specific data types and values

The Directory can be better understood as a specialized distributed database, whose stored data or information has both an **internal** and **external** structure.

## Internal Directory Structure

The internal structure is generally referred to as the **schema**. The schema describes the relationships between the different **types** of objects that can be stored in the Directory. A type of object could be an organization, meeting room, device, person, program, or process.

The basic data item stored in the Directory is an **entry**. An entry represents a physical entity (for example, Meeting Room 07CA) that may belong to one or more object classes. Each object class is a collection of related attributes. For example, the meeting room capacity could be an attribute of the physical entity, Meeting Room 07CA. Attributes themselves can be single valued or multivalued. Thus to describe a physical entity, the attributes are given values. For example, if the capacity of Meeting Room 07CA is 10 people, the attribute value is 10.

Each entry in the Directory has a unique name, the DN. The DN uniquely identifies the position of an entry in the hierarchical structure. Thus the external structure of the Directory is the structure of names that the user sees; for example, the organization chart.

### External Directory Structure

The external structure of names is called a **namespace**. It is this namespace capability of the Directory that is particularly suited to describing hierarchically structured organizations.

Potentially, a Directory can also describe subjects and objects. When this is the case, some subjects or groups of subjects can access all or a portion of the information about an object. For example, continuing the illustration of Meeting Room 07CA, the people authorized to obtain information about the meeting room are the directory subjects. Your organization's Directory should provide access control mechanisms to implement such a requirement.

## Web Browser and Server Communications

A Web browser enables a user to browse the Web or local HTML pages. It is basically a retrieval tool that provides universal access to the vast collection of materials available on the Web and Internet. Examples are Netscape Navigator, Netscape Communicator, and Microsoft Internet Explorer.

SSL is a protocol developed by Netscape Communications Corporation that provides secure communication between a Web browser and server. It supports server and client authentication. SSL is application independent, allowing protocols such as HTTP, FTP, and Telnet to be layered on top of it transparently.

SSL is able to negotiate encryption keys as well as authenticate the server before data is exchanged by the higher-level application. It uses encryption, authentication, and message authentication codes to maintain the security and integrity of the transmission channel.

The SSL protocol supports a variety of cryptographic and hash algorithms including **RSA** (named for its inventors Rivest, Shimer, and Adelman) and **MD5** (message digest version 5). The public key certificates follow the X.509 syntax.

## Vault Agent

The Vault Agent incorporates a small subset of vault process functionality to provide non-Web based interaction with the Vault Controller. This subset enables the Vault Agent to exchange secure messages with vaults running under the control of the Vault Controller or another Vault Agent. For example, your organization’s software applications can use the Vault Agent to request and receive certificates for customers and employees at remote locations.

## Vault Agent Application

The following graphic depicts the structure of a Vault Agent application:

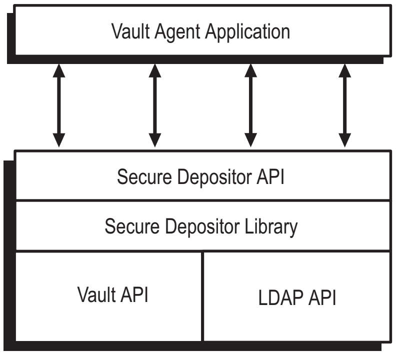


*Figure 7. Vault Agent Application Structure*

Your organization’s custom Vault Agent application sits directly on top of the Secure Depositor **application program interface** (**API**). The Secure Depositor uses the LDAP library to access the Directory and the Vault APIs to perform encryption, decryption, signing, and verification functions. The keys these functions use reside (in encrypted form) in a profile stored on the Vault Agent. A password must be supplied at start-up to allow the Vault Agent to access the private keys in the profile.

## Vault Agent Operation

The main function of a Vault Agent is to send messages to, and receive messages from, vault processes running on the Vault Controller. Messages are signed and encrypted before transmission. A TCP/IP socket connection is used to transmit messages from the Secure Depositor process to a Secure Depositor daemon.

The Secure Depositor takes the DN of a target vault owner as an argument; for example, `CN=CA1,ou=VReg,o=IBM,c=US`. It accesses the appropriate record from the Directory and extracts the `comment` attribute. The `comment` attribute contains a signed message which is a combination of:

- Vault owner DN ("`CN=CA1,ou=VReg,o=IBM,c=US`")
- Vault ID (vault name)
- Vault path ("`/local/vaults`")
- Vault IP address
- Vault encryption level

Combining the vault owner DN and the vault name in the signed message provides two benefits. The first benefit is that the Secure Depositor can verify that the vault name is actually bound to the user DN and this binding has not been modified. The second benefit is that if someone has replaced the signed message in the user DN record with that from another record, the user DN in the signed message will not match the DN in the Directory record. The Secure Depositor will then reject the encryption attempt.

The following graphic depicts an example of an interaction between a Vault Agent and a vault process.

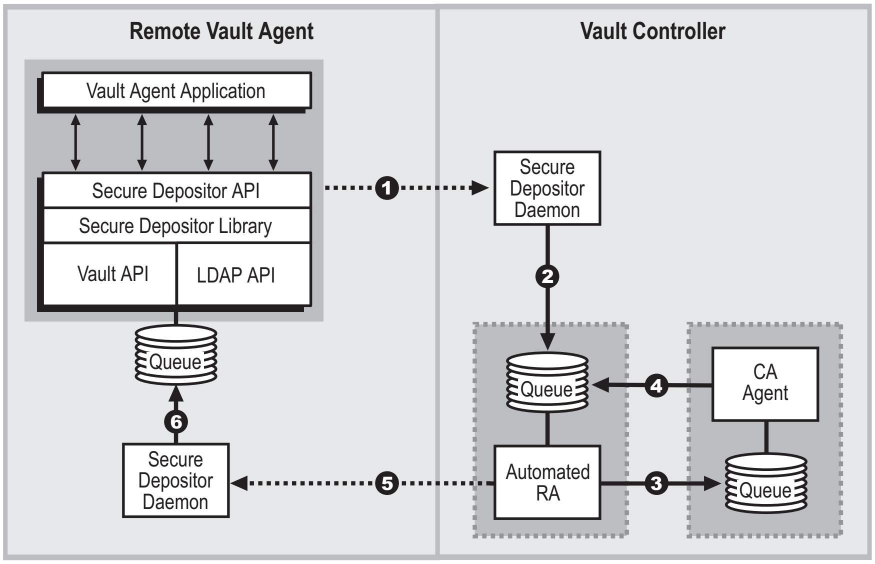


Figure 8. Vault Agent and Vault Process Interaction

The remote vault process in this case is an automated RA that accepts requests including those to certify public keys and renew certificates. The automated RA, in turn, communicates with a local vault process (known as a CA Agent) which deals with the CA to carry out the RA requests.

- In steps 1 and 2: the Vault Agent sends a request to an automated RA to issue a certificate.
- In step 3, the automated RA verifies the signature of the incoming record and forwards the request to the CA Agent after creating appropriate audit records.
- In step 4, the CA Agent signs the certificate – through the CA – and returns it to the automated RA.
- In steps 5 and 6, the automated RA sends the certificate back to the remote Vault Agent. The remote Vault Agent then delivers it to the appropriate user.

**Note:** To use the Vault Agent with the Vault Registration Application, the Vault Agent must be enrolled in the ACL for the Master RA. For more information, refer to the *Vault Registration Application for AIX Customization Guide*.

# Chapter 3. Supported Standards

This chapter lists the security standards that IBM Vault Registry supports or complies with and the different encryption levels used in a Vault Registry system.

## Security Standards

The three major components of Vault Registry — Vault CMS, the Directory, and the Vault Controller — comply with or support the standards described in the following table.

| | |
|---|---|
| Vault Controller | Secure Sockets Layer versions 2 (SSLv2) and 3 (SSLv3) with client authentication |
| | Standards PKCS #7 and PKCS #10 |
| | Client certificate requests for Microsoft Internet Explorer, Netscape Navigator and Netscape Communicator |
| | Server certificate requests for Netscape Enterprise Server, IBM Internet Connection Secure Server, and Microsoft Internet Information Server |
| | Server certificate requests using RFC 1424 Privacy Enhanced Mail |
| Vault CMS System | X.509v3 certificates |
| | CA key length of 1024 bits |
| | Browser certificates for 512, 768, and 1024 bit keys |
| | Signature certificates for 1024-bit keys |
| | Encryption certificates for 512- through 1024-bit keys |
| | Hash algorithms MD5, SHA-1 |
| | Certificate revocation lists (CRLv2) |
| | LDAP for directory communications with the Directory |
| Directory | LDAP Version 2.0 with RFC 1779 syntax for communications by the CA and other components |

The Vault Registry hardware components — the 4758 and CCA Cryptographic Coprocessor Support Program — comply with or support the standards described in the following table.

| | |
|---|---|
| IBM 4758 PCI Cryptographic Coprocessor | FIPS 140 level 3 requirements for resistance to physical attacks |
| | Industry cryptography standards: |
| | - DES for encryption/decryption |
| | - RSA for signing/signature verification |
| | - PKCS #1 block type 00, PKCS #1 block type 01, and PKCS #1 block type 02 |
| | - Hash algorithms: MD5, SHA-1 |
| | - ANSI X9.9, X9.23 |
| | - ISO 9796 |

| | |
|---|---|
| IBM CCA Cryptographic Coprocessor Support Program | Full capabilities of the IBM 4758 providing services including the secure generation of RSA key pairs with modulus lengths as long as 2048 bits: |
| | - SET (Secure Electronic Transaction) |
| | - DES for encryption and decryption |
| | - RSA for signing and signature verification |
| | - Hash algorithms MD5, SHA-1 |

## Encryption Levels

To comply with export regulations, the version of IBM Vault Registry determines the encryption level available to Vault Registry applications. This is true whether the system is at your site or at the site of any vault your application needs to access. These cryptographic algorithms are predetermined and your site cannot alter them when it configures Vault Registry.

Each component in the Vault Registry technology that is involved in secure messaging has a variable that identifies the highest allowable encryption level. The encryption levels used in a Vault Registry system are: **triple Data Encryption Standard** (**DES**) for the Strong encryption edition and DES for the International edition. Embedding the encryption level in the code, rather than providing encryption options in the APIs presented to applications, guarantees that the Vault Registry technology uses only the predefined algorithms.

When the Secure Depositor searches for the record of the recipient user DN, it verifies the signature in the `comment` attribute. If the signature is verified and the user DN in the signed message matches the record user DN, it extracts the encryption level of the recipient vault from the `comment` attribute. It uses simple conditional logic to select the encryption level: that is, it uses the highest level of encryption common between the sender and recipient.

Refer to the following table for a summary of the encryption algorithms.

| **Sender** | **Strong Recipient** | **International Recipient** |
|---|---|---|
| Strong | Triple DES | DES |
| International | DES | DES |

# Chapter 4. System Requirements

Your operating environment must meet the hardware and software requirements discussed in the following sections. For the latest information, see the *Readme* file distributed on the *IBM Vault Registry code for AIX* product CD-ROM. That file, available as text or HTML, contains the latest additions and changes to the requirements and procedures in this book.

## Required Server Hardware

The Vault Registry product has been verified for the following hardware configurations:

- IBM RISC System / 6000® (RS / 6000®):
  - Model 7017–S70, 4–, 8–, or 12–way SMP (specify machine type 7013–J40 or 7015–R40 if upgrading)
  - Model 7025–F50, 1– to 4–way deskside SMP
  - Model 7026–H50, 1– to 4–way rack SMP

The following table provides system sizing recommendations based on the number of certificates you expect to issue through a Vault Registry certificate authority.

| Development Environment | Processors | RAM | Disk Space |
|---|---|---|---|
| **Small**: may issue hundreds of certificates per day, primarily for use in development and test activities (570 processor level — not a production environment) | 2 | 512 MB | 9 GB |
| **Medium**: may issue thousands of certificates per day (J40 processor level) | 4 | 1 GB | 18 GB |
| **Large**: may issue many thousands of certificates per day (S70 processor level) | 8 | 1 GB | 18 GB |

## Optional Server Hardware

For added security of CA keys, the following cryptographic adapter is an optional but recommended component:

- IBM SecureWay 4758 PCI Cryptographic Coprocessor, Model 001

  If used, you must order this product through normal IBM hardware ordering channels. You must also install it on the server where you plan to install IBM Vault Registry before you install the Vault Registry server components. Note that this card requires a PCI bus on the RS / 6000.

## Required Server Software

The Vault Registry product has been verified with the following corequisite products:

- IBM AIX / 6000® operating system, version 4.3.2

  See the *Readme* file for the latest information about supported versions and required software patches.
- Lotus Domino Go Webserver, version 4.6.2

  A version of Domino Go specific to an encryption level and language is included in the Vault Registry product distribution package. You must install this software on the same server where you install the Vault Controller.

- A Directory product, such as:
  - IBM eNetwork X.500 Directory, version 1.0.1
  - IBM eNetwork LDAP Directory, version 2.1

  You can order these products through normal IBM software ordering channels, or use third-party software that provides PKI-compliant Directory support. You can install the Directory on the same server where you install the Vault Controller or on a remote AIX server.
- IBM DB2 Universal Database Enterprise Edition for AIX, version 5.0

  You must order this product through normal IBM software ordering channels. You can install DB2 UDB on the same server where you install the Vault Controller or on a remote AIX server.

## Optional Server Software

If you plan to install the optional 4758 PCI Cryptographic Coprocessor, then the following software is required:

- IBM 4758 CCA Support Program, version 1.3.0.0

For network management and monitoring, the following software is an optional but recommended component:

- IBM Tivoli TME 10 NetView™, version 5.0

If used, you must order these products through normal IBM software ordering channels and install them on the same server where you install the Vault Controller.

## Required Client Hardware

If used, you must install the Vault Agent and Vault Certificate Validator components on either an IBM AIX or a Microsoft Windows NT platform.

IBM AIX requirements:

- RS/6000, such as a model 7020 with a CD-ROM drive
- Graphics card
- VGA video display (or better)
- Mouse or mouse-compatible pointing device

Microsoft Windows NT requirements:

- Personal Computer with at least a 486/66 microprocessor and a CD-ROM drive
- Graphics card
- VGA video display (or better)
- Mouse or mouse-compatible pointing device

## Required Client Software

If you install the Vault Agent and Vault Certificate Validator client components, one of the following operating systems is required:

- IBM AIX/6000 version 4.3.2
- Microsoft Windows NT version 4.0

You must also install one of the following Web browsers:

- Netscape Navigator or Netscape Communicator version 4.0 or later
- Microsoft Internet Explorer version 4.0 or later

  The end-user features have also been tested with Netscape Navigator version 3.0 for the International encryption level.

## Vault Registry Applet Requirements

The following applets, which were created with the Sun Java programming language, are included in the Vault Registry product:

- The Configuration applet enables administrators to configure the system components after installing the software.
- The RA Desktop applet enables Master RA users and RA administrators to process enrollment requests and manage certificates throughout their life cycle. When the applet is loaded, title information indicates whether it is being run by a Master RA user or an RA administrator.

To run these applets, you must install one of the following Web browsers on a Windows platform:

- Netscape Navigator or Netscape Communicator, version 4.05 or later
- Microsoft Internet Explorer, version 4.0 or later, with Java enabled and HTTP 1.1 disabled

You must install the official version of the product as distributed by Netscape or Microsoft. Versions obtained from third-party vendors may not display information correctly, especially when running the applet in a language other than English.

## Application Development Requirements

If your enterprise plans to develop or integrate applications using the APIs provided for the Vault Controller, Vault Agent, or Vault Certificate Validator, the following compilers are recommended:

- In an IBM AIX application development environment: IBM C Set ++ for AIX version 3.1 or later
- In a Microsoft Windows NT application development environment: Microsoft Visual C++

# Chapter 5. Vault Registry Applications and Scenarios

There are many potential business applications for the Vault Registry product. The following table lists typical industries (acting as CAs), the secure business applications they might run, and the users they might certify to access those applications.

| CAs | Business Applications | Certified Users |
|---|---|---|
| Financial institutions, banks | Secure payment transactions | Merchants, cardholders |
| Banks | Home banking, loan and mortgage processing | Account holders |
| U.S. Federal Government, state governments | Filing tax returns, applying for and acknowledging social security benefits | Citizens |
| | Filing financial reports with SEC (Securities Exchange Commission) | Businesses |
| Postal agencies | E-postmarks, e-registered mail | Postal customers |
| Health insurance companies, HMOs, AMA (American Medical Association) | Accessing patient records, filing treatment plans, securing treatment authorizations, obtaining reimbursement for services performed | Physicians, hospitals |
| Legal agencies and courts | Filing court affidavits and other legal documents | Judges, lawyers, paralegals |
| Internet service providers (ISPs) | Dial-up account access | Businesses using ISP services |
| Software businesses | Making sure software being downloaded is protected against viruses | Software modules |
| | Delivering and supporting electronic software | Customers |

The many potential business applications for the Vault Registry product are best described using true-to-life business situations (or scenarios). Therefore, this chapter provides two scenarios. Each scenario describes the use of Vault Registry technology in a particular business arena: one arena is home banking, and the other is health care services. Both scenarios give the steps an applicant would follow and the behind-the-scenes processing that would occur on the Vault Controller when a certificate is issued.

## Scenario 1: Registering for Home Banking

This scenario describes the registration process for an applicant for a bank’s services. The process includes the creation of a vault and the receipt of an organization certificate for accessing bank services. All keys and certificates in this scenario are stored in the applicant’s browser.

RA activities include management of an automated RA by the RegistryVault Bank vault CA for creating vaults, and operation of an organization RA administrator by bank personnel for approving requests and issuing organization certificates from the bank CA.

Figure 9 illustrates the following process of setting up home banking:

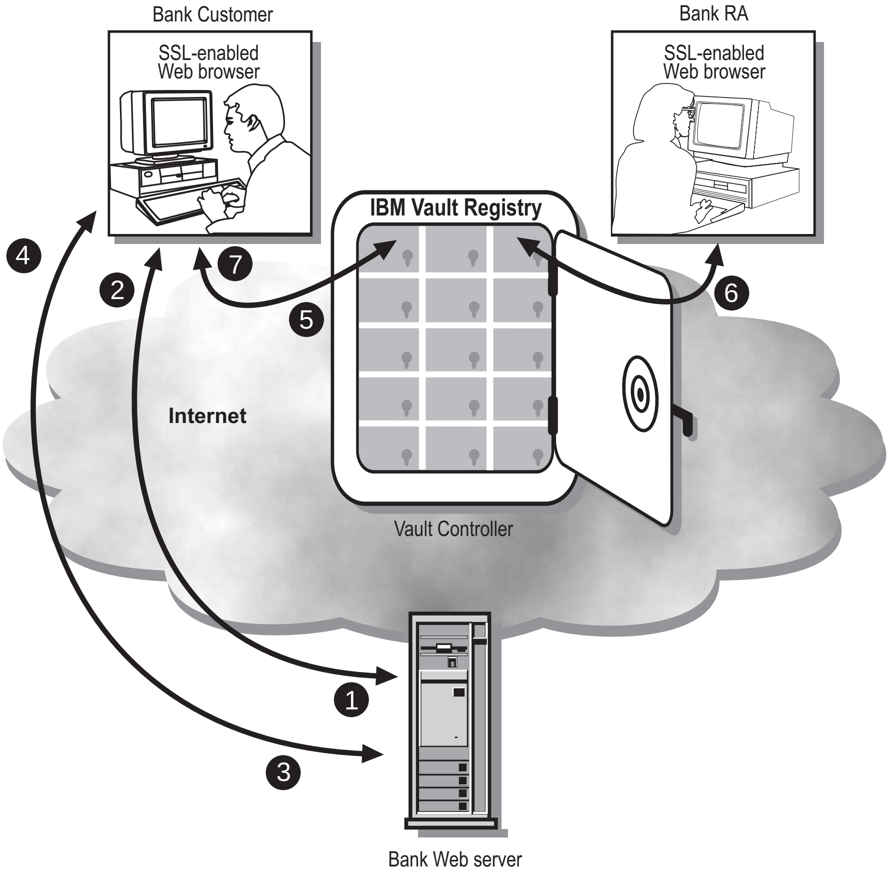


*Figure 9. Setting Up Home Banking*

1. The bank customer accesses a registration form from the bank’s URL.
2. The bank customer receives and completes the registration form.
3. The bank customer submits the registration form to the bank.
4. IBM Vault Registry returns a vault access certificate that allows the customer access to a vault on a Vault Controller.
5. The bank customer uses the vault access certificate to gain access to a vault on the Vault Controller in order to determine the status of the registration request.
6. The bank’s RA administrator approves the certificate request.
7. The bank customer downloads the organization certificate to the browser and uses it to access the bank’s services.

## Introduction

RegistryVault Bank decides to offer home banking. They use Vault Registry technology to issue certificates to access their home banking application.

John, a new customer, decides to open an account at RegistryVault Bank. The RegistryVault Bank customer service representative gives John a RegistryVault

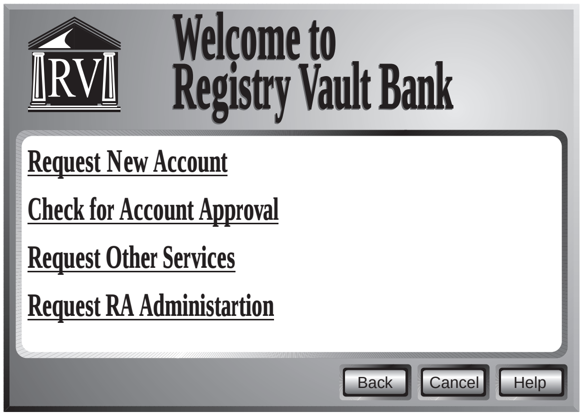
Bank Internet banking brochure, which describes the benefits of Internet banking and the information he needs to request home banking. Excited about the technology and convenience, John decides to open his home banking account.

The process of registering John for home banking includes the following basic steps:

1. Requesting an account
2. Checking credentials and registering the new account
3. Receiving the new account

## Requesting an Account

1. John reads the RegistryVault Bank Internet banking brochure. Then, following the directions in the brochure, he opens his Web browser and accesses the RegistryVault Bank home page:



Welcome to Registry Vault Bank

Request New Account

Check for Account Approval

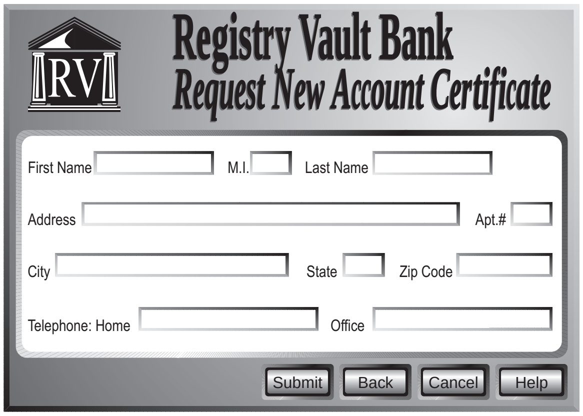
Request Other Services

Request RA Administartion

*Figure 10. RegistryVault Bank Home Page*

**Note:** John’s browser displays an icon indicating that he does not have a secure session while accessing the page. Some versions of Netscape display an unlocked padlock (or broken key) to indicate a non-secure Web session. They display a locked padlock (or unbroken key) to indicate a secure Web session. Other browsers use different icons.

2. John clicks `Request New Account`. RegistryVault Bank displays its form for requesting a certificate for a new online account.



Registry Vault Bank
Request New Account Certificate

First Name M.I. Last Name

Address Apt.#

City State Zip Code

Telephone: Home Office

*Figure 11. RegistryVault Bank Online New Account Request Form*

3. John fills out the application form, providing potentially sensitive information such as address and telephone numbers. He then submits the form, and the following process takes place:
   a. The RegistryVault Bank generates a key pair and sends the public key with the form.
   b. John's browser displays an icon to indicate that RegistryVault Bank is providing a secure Web session for transmitting his registration information to the Vault Controller.
   c. Vault Registry runs within the Vault Controller.
   d. John's application form is submitted to a common vault known as the validator vault.
   e. The validator vault application checks the contents of the form and, if the contents are valid, tells the browser to generate a new key pair.
   f. The public key is sent to the validator.
   g. The validator creates a vault.
   h. The application sends a vault access certificate to John's browser for storage.
   i. The application sends the application form to the appropriate RA administrator.
4. John presents his vault access certificate to access his vault and start the vault application that checks the status of his RegistryVault Bank certificate request. The vault application processes John's request for certificate status. If the request has not yet processed, a message displays on an HTML page to John's browser indicating that the request is pending.

## Checking Credentials and Registering the New Account

Bill is a RegistryVault Bank RA administrator. He reviews new account request forms.

The RA administrators at RegistryVault Bank have been certified by RegistryVault Bank CAs using the Vault Registry product. Therefore, each RA administrator has a vault and vault access certificate.

1. At his workstation, Bill accesses the RegistryVault Bank home page and clicks on `Access RA Administration`.
2. After Bill clicks on `Access RA Administration`, his browser prompts him for his vault access certificate.

The request to perform RA administration tasks is sent to the Vault Controller and routed to Bill’s vault. The application in Bill’s vault generates a Web page which is sent to Bill’s browser.

Bill then sees the `RA Administration` home page:

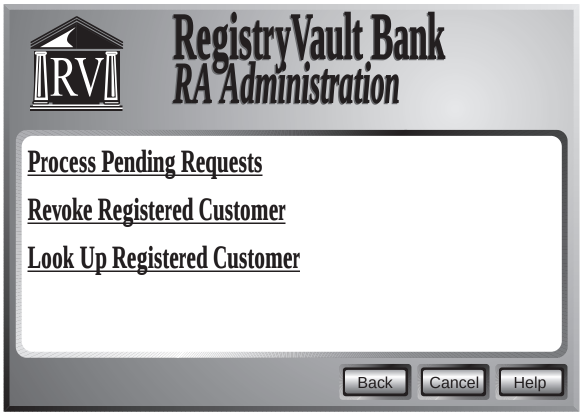


*Figure 12. RegistryVault Bank RA Administration Home Page*

The `RA Administration` home page contains the following links:

```
Process Pending Requests
Revoke Registered Customer
Look Up Registered Customer
```

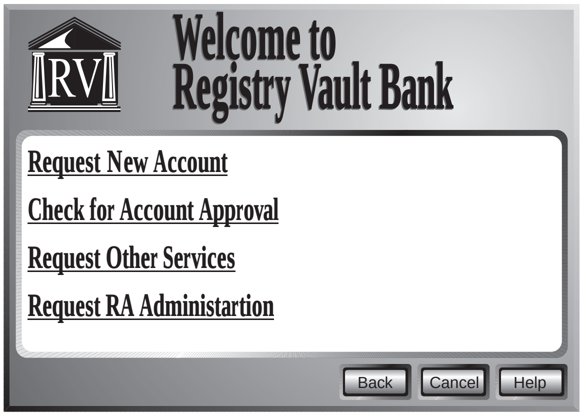
3. Bill clicks `Process Pending Requests`. The Vault Controller runs an application in Bill’s vault which generates a Web page with links for all pending requests that have been sent. This page is then sent to Bill’s browser.
4. Bill clicks the first link (John’s registration form). A request is sent to the Vault Controller. The application then decrypts John’s request form, which was encrypted with Bill’s public key, and displays it to Bill’s browser for review.
5. Bill checks John’s account and, according to the bank’s policies, completes RegistryVault Bank’s Applicant Review form to document his evaluation.
6. Satisfied with John’s credentials, Bill clicks `Approve Request` at the bottom of the form.

   This executes an application in Bill’s vault that signs John’s public key and creates John’s RegistryVault Bank certificate.

   **Note:** The time required for the approval process varies depending on a number of factors such as network delays, the issuing organization’s policy, and current applicant demand.

## Receiving the New Account

1. John returns to the RegistryVault Bank home page later that afternoon and accesses his vault after presenting his vault access certificate. A software application launches in his vault to check his request status. Because his request has been accepted and because he requested notification, an approval message is generated and sent back to John’s browser.
2. John follows the browser’s instructions to download the certificate.
3. After downloading the certificate, John’s browser again displays the RegistryVault Bank home page.



Welcome to Registry Vault Bank

Request New Account

Check for Account Approval

Request Other Services

Request RA Administartion

*Figure 13. RegistryVault Bank Home Page: Request Other Services*

John is now ready to use his new certificate to bank from home.

4. John clicks `Request Other Services`.
5. The browser prompts John to select a certificate. John has two types of certificates in his browser: a vault access certificate and the RegistryVault Bank certificate. John selects his RegistryVault Bank certificate and clicks `OK`.
6. The browser displays the message:

   ```
   Welcome. You have accessed RegistryVault Bank.
   ```
7. John has accessed the RegistryVault Bank server — securely — and can access any of the RegistryVault Bank applications running on this server:
   - `Checking`, to obtain his checking account balance or confirm the date of the last deposit to his checking account
   - `Savings`, to obtain his savings account balance, check the amount of interest his savings account has accrued, or confirm the date of the last deposit to his savings account
   - `Bill Payment`, to initiate payment of his telephone, utility, or credit card bills
   - `Credit Cards`, to check the credit line, available credit, or total due on his credit cards

**Note:** The home banking scenario described in the preceding text is an application that a customer can write and run on any application Web server. The secure Web server platform used by Vault Registry is one option. The certificates issued by the Vault Registry Vault Registration Application, however, can be used successfully with any other application Web server that supports X.509v3 certificates.

## Scenario 2: Registering for Health Care Services

This scenario describes the registration processes for applicants for specific online health care services. All processes include the receipt of certificates for providing and receiving health care services. All keys and certificates in this scenario are stored in the individual browser of each applicant.

### Introduction

Any person or entity that wants to provide health care in the state — doctors, pharmacists, or other health care providers — must be approved by the State Medical Board before they are licensed to legally provide services. The Medical

Board processes all applications for licenses. When the board approves an application, it registers the applicant as an authorized provider of care and updates its databases. When it rejects an applicant, it notifies the applicant and posts a rejection record in its database.

The Medical Board supports digital certification of its licensed practitioners where a licensee is issued a signed digital certificate. The certificate policies that are defined and maintained by the Medical Board specify the ways a licensee can use the certificate. These policies link the use of the certificate to the kind of medical care and service the person or entity may provide or receive. For example, a pharmacist would be allowed to dispense the medication requested in a prescription — deliver it to the patient — but the pharmacist would not be able to write the prescription.

Patients who wish to use this new technology — electronically request refills of their prescriptions, for example — register with health care providers. All health care providers have been licensed by the State Medical Board to offer electronic health care management services. One such provider is RegistryVault HealthCare. RegistryVault HealthCare uses Vault Registry technology to issue certificates that allow patients to request a number of services from home, including prescription medication refills.

James decides to use this technology by registering with RegistryVault HealthCare. The RegistryVault HealthCare customer service representative gives James a RegistryVault HealthCare Internet brochure that describes the benefits of Internet health care services and the information he needs to register.

The process of registering James for health care services with RegistryVault HealthCare and then receiving some of those services includes the following steps:

1. Registering RegistryVault HealthCare
2. Registering the doctor
3. Registering the pharmacist
4. Registering the patient
5. Checking credentials and registering the new account
6. Receiving the account
7. Requesting a prescription refill
8. Filling the prescription

## Registering RegistryVault HealthCare

To recruit health care providers and patients to obtain or provide medical services in the state, RegistryVault HealthCare should be authorized to do so by the State Medical Board. In this scenario, the State Medical Board also authorizes RegistryVault HealthCare to electronically register and certify its participating members by authorizing them to operate as a Registration and Certificate Authority. The State Medical Board uses Vault Registry to register HMOs such as RegistryVault HealthCare, licensing them to register people or entities that want to receive or provide medical services.

## Registering the Doctor

Before participating in RegistryVault HealthCare's HMO program, doctors must be affiliated with the HMO. This is an offline process in which the doctor and

RegistryVault HealthCare come to an agreement to work together. As part of the process, RegistryVault HealthCare enters the required information about the doctor in its database and allows the doctor to participate in the program.

Dr. Smith has participated in RegistryVault HealthCare's network for a few years. As an active member, she receives a brochure from RegistryVault HealthCare on its new online Internet health care provisions. As it offers many advantages over traditional services, she decides to enroll in the program.

1. Dr. Smith invokes the Internet browser on her machine and types the URL specified in the brochure to get to RegistryVault HealthCare's site. The session is an unsecured session. As she scrolls down the home page for RegistryVault HealthCare, the doctor sees the following options:

   ```
   Click here if you are an affiliated doctor
   Click here if you are an affiliated pharmacist
   Click here if you are an affiliated patient
   ```

2. Dr. Smith clicks the first option to access the Web server that hosts the health care application. RegistryVault HealthCare only allows participants certified by the board or by itself to access this Web site. Before allowing the application to run, the Web server prompts Dr. Smith with a Web page containing the following options:

   ```
   Click here if you have a digital certificate from the State
   Click here to get a digital certificate from the State
   ```

3. Since this is the first time that Dr. Smith has accessed the Web site of RegistryVault HealthCare, she does not have a certificate from the State Medical Board. She clicks the second option. The second option links to the State Medical Board's Web site. The digital certificate issued here is through Vault Registry.
4. At the State Medical Board site, the doctor is prompted to register through Vault Registry. The flexibility of Vault Registry allows the Medical Board two options in dispensing a certificate:
   - Direct enrollment, where the doctor downloads the certificate from a central server using challenge and response authentication
   - Vault-based enrollment, where the doctor applies for and receives certificates in strongly authenticated end user vaults.

   The State Medical Board has implemented the direct enrollment method in this case.
5. Dr. Smith is asked to complete a registration form customized by the State Medical Board which includes the doctor's license number. The RA administrator at the Medical Board reviews the application, and once satisfied, approves the doctor. This approval prompts the CA to issue a digital certificate to Dr. Smith. The digital certificate has the doctor's license number in the Distinguished Name field.
6. Dr. Smith now returns to RegistryVault HealthCare's Web site. While she is connecting, the Web server requests her certificate and she selects the one provided by the State Medical Board. This certificate is recognized (trusted) by RegistryVault HealthCare. The Web server allows her to access the application. The application extracts the license number from the Distinguished Name field of the certificate and tries to find a match in its database of affiliated doctors. It finds a match and checks to see if Dr. Smith is already approved to use its online services. If not, it approves Dr. Smith and allows her access to the services she can use within the organization's policy structure.

**Note:** The database at RegistryVault HealthCare can store more than just information about Dr. Smith. It can be the repository of information such as the list of patients who want to contact her. It can also be prescription refills that require approval and links to patient records the doctor may have requested.

## Registering the Pharmacist

The registration process for the pharmacist, Sam Jones, is the same as the process for the doctor. The pharmacist should also be affiliated with RegistryVault HealthCare before registering with the HMO online.

## Registering the Patient

Just like Dr. Smith and Sam Jones, James should be affiliated with RegistryVault HealthCare before using its services. This may happen in many ways – in this case, James hears of RegistryVault HealthCare through his employer. He completes a standard application form and submits it to his employer who, in turn, sends it to the HMO for approval. Once approved, James is sent a brochure on online health care that the HMO provides. He also receives a one-time password to use if he decides to register online.

1. James sits down at his Web browser and reads the RegistryVault HealthCare Internet health care services brochure. Following the directions in the brochure, he opens his Web browser and accesses the RegistryVault HealthCare home page. James selects `Click here if you are a patient` to display the RegistryVault HealthCare online application form. He completes and submits the form.
2. James is prompted with the following options:

   ```
   Click here if you are registered
   Click here if this is your first time visiting our site
   ```

   He clicks on the second option which leads him to the registration page. He completes and submits the form. As part of the registration process, he receives a prompt to enter the one-time password that was provided to him.

   **Note:** The information that James provided in his application included a secret PIN and potentially other medical information. However, he does not need to worry about unauthorized entities accessing the information because IBM Vault Registry allows RegistryVault HealthCare to provide a more secure environment for transmitting his sensitive information.

   Vault Registry provides more than just a secure Web session. It encrypts the applicant's information during transmission and storage, and prevents any unauthorized access to that information. No one can access this information except James and the parties specifically authorized to process his request. Not even the system operators and administrators have this authority.
3. James's application form undergoes an initial validation process. When it successfully completes this process, James receives a temporary access certificate that allows him to check the status of his request for access to RegistryVault HealthCare services. This access certificate allows him to enter his user vault within Vault Registry. James checks the status of his request but the request has not yet been processed; a message is returned to James's browser indicating that the request is pending.

## Checking Credentials and Registering the New Account

Tom is a RegistryVault HealthCare RA administrator. He reviews new registration request forms. One of Tom's responsibilities is to process pending applications. The first application that Tom retrieves from the queue of waiting applications is the one that James submitted. Vault Registry decrypts James's request form and displays it to Tom's browser for review. Only authorized RAs at RegistryVault HealthCare, like Tom, are allowed to view this information.

1. Tom checks James's employment and payment status and completes RegistryVault HealthCare's `Applicant Review` form to document his evaluation.
2. Satisfied with James's credentials, Tom clicks `Approve Request` at the bottom of the form. This action prompts the certificate management entity within Vault Registry to issue a digital certificate to James. This certificate authorizes James to use the services to which he is entitled governed by the company's policies.

## Receiving the Account

1. James returns to the RegistryVault HealthCare home page later that afternoon and checks the status of his request. He finds that his request has been accepted. He has received a certificate that allows him to access the specific RegistryVault HealthCare services he requested.
2. John follows the browser's instructions to download the certificate.
3. After downloading the certificate, James's is ready to use RegistryVault HealthCare services. He decides to use his new certificate to request a prescription refill.
4. James goes to the RegistryVault HealthCare home page and clicks `Request Prescriptions`.
5. The browser prompts James to select a certificate. One of the certificates in his browser is the RegistryVault HealthCare certificate. James selects his RegistryVault HealthCare certificate and clicks `OK`.
6. The browser displays the message:

   ```
   Welcome. You have securely accessed RegistryVault HealthCare and can now securely
   use RegistryVault health care services.
   ```
7. James has accessed the RegistryVault HealthCare server — securely — and can now access any of the RegistryVault HealthCare applications running on this server.

## Requesting a Prescription Refill

1. James clicks `Refill Prescription`. He enters the following information in the request form that is displayed:

   ```
   Name and address of patient
   Name and address of doctor
   Name of medication and amount required
   ```
2. For the `Send Prescription To` option, James selects `Doctor`. He clicks `Submit` to transmit his request to his doctor, Dr. Jane Smith. The request is sent to Dr. Smith, who is a registered provider through RegistryVault HealthCare. The RegistryVault HealthCare application processes the request.
3. Dr. Smith checks James's medical history, latest test results, and the most current information on the medication.
4. Satisfied that James's condition warrants a refill of the same medication, Dr. Smith enters the medication information that is needed. She then approves the prescription refill request. Depending on the type of application, Dr. Smith may digitally sign the request form to authenticate her approval.

**Note:** In many states, Dr. Smith's digital signature has the same legal standing as her physical signature. Therefore, the digitally signed request form is a legal document just as a hardcopy prescription would be.

## Filling the Prescription

1. When Dr. Smith clicked `Approve Request` to create James's prescription refill request, the RegistryVault HealthCare application sent the request to Sam Jones at Jones Pharmacy, the pharmacist authorized to fill the prescription.
2. The personnel at Jones Pharmacy do not personally know either Dr. Smith or James. However, when they receive the prescription, they accept the digital signatures of Dr. Smith and James. They accept Dr. Smith's signature because it has been certified by their state's Medical Board. They accept James's signature because it has been certified by RegistryVault HealthCare who has been certified by the State Medical Board.
3. The personnel at the pharmacy complete the processing of the refill request and notify James that his prescription is ready.

**Note:** The prescription refill scenario described in the preceding text is an application that a customer can write and run on any application Web server. The secure Web server platform used by Vault Registry is one option. The certificates issued by the Vault Registry Vault Registration Application, however, can be used successfully with any other application Web server.

# Glossary

This glossary defines terms and abbreviations used in this book that may be new or unfamiliar and terms that may be of interest. It includes terms and definitions from:

- The IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- The American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

# Numbers

**4758 PCI Cryptographic Coprocessor.** A programmable, tamper-responding cryptographic PCI-bus card offering high performance DES and RSA cryptographic processing. The cryptographic processes are performed within a secure enclosure on the card. The card is designed to meet the stringent requirements of the FIPS PUB 140-1 level 4 standard. Software can run within the secure enclosure. For example, credit card transactions can be processed via the SET standard.

# A

**Abstract Syntax Notation One (ASN.1).** This is an ITU notation used to define the syntax of information data. It defines a number of simple data types and specifies a notation for identifying these types and for specifying values of these types. These notations can be applied whenever it is necessary to define the abstract syntax of information without curbing how the information is encoded for transmission.

**access control list (ACL).** A mechanism for limiting use of a specific resource to authorized users.

**ACL.** Access control list.

**American National Standard Code for Information Interchange (ASCII).** The standard code used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set uses a coded character set consisting of 7-bit coded characters (8 bits including parity check) and consists of control characters and graphic characters.

**American National Standards Institute (ANSI).** An organization that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. It consists of producers, consumers, and general interest groups.

**ANSI.** American National Standards Institute.

**API.** Application program interface.

**applet.** A computer program that is written in Java and runs inside a Java-compatible browser such as Netscape Navigator. Also known as a Java applet.

**application domain.** A unique implementation of a Vault Registration Application. Each domain defines a set of resources, policies, and configuration options related to specific certificate registration processes. All Vault Registration Application functions base their processing on application domain definitions. The domain name uniquely identifies the application to the Vault Controller.

**application program interface (API).** In Vault Registry, a functional interface that allows an application program written in a high-level language to use specific Vault Registry functions.

**application state.** In Vault Registry, the status of a request that is tracked in a Vault Registration Application database. For example, the state of an application changes from `Application Pending` to `Application Approved` when an RA approves the application. States and state changes are important to the Recovery Agent.

**ASCII.** American National Standard Code for Information Interchange.

**ASN.1.** Abstract Syntax Notation One.

**asymmetric cryptography.** Cryptography that uses different, asymmetric keys for encryption and decryption. A pair of keys is assigned to each user: a public key accessible to all, and a private key known only to the user. A secure business transaction can occur when the public key and the corresponding private key are matched, enabling the decryption of the transaction. This is also known as key pair cryptography. *Contrast with* symmetric cryptography.

**asynchronous communication.** A mode of communication that does not require the sender and recipient to be present simultaneously.

**audit trail.** Data, in the form of a logical path that links a sequence of events. An audit trail can be used to trace transactions or the history of a given activity. For example, it may track activity in a customer account.

**Authcode.** An authorization code that is used along with a reference ID to access an Entrust-ready VPN product. Users enroll and apply for a RefID and Authcode pair through the Vault Registration Application.

**authentication.** The process of reliably determining the identity of a communicating party.

**authorization.** Permission to access a resource.

**automated RA (Auto RA).** A vault process that immediately processes requests for certification. After receiving a request for a certificate, an Auto RA automatically approves it, issues the certificate, and returns it to the requestor. An Auto RA allows organizations to maintain control over user registration while offloading the certificate management process.

## B

**browser.** *See* Web browser.

**browser certificate.** A digital certificate, also known as a client-side certificate, issued by a CA through an SSL-enabled Web server. The keys that enable the holder of the certificate to encrypt, decrypt, and sign data are typically stored in an encrypted file by the Web browser. Some applications permit the keys to be stored on smart cards or other media. In a Vault Registry system, browser certificates are obtained through the Vault Registration Application. *See also* digital certificate.

## C

**CA.** Certificate authority.

**CA Agent.** A local vault process that interacts with the CA to carry out requests for certificate management services.

**CA site certificate.** A certificate that has not been signed by a recognized CA. When installing the Web server, an administrator must follow the procedures for that server to generate a public/private key pair and self-signed site certificate. (For some Web servers, such as Netscape, the CA site certificate is provided automatically.) After installing the site certificate, the administrator can use the Vault Registration Application to obtain a server certificate that is signed by a trusted CA. This enables requests that use the SSL protocol to be authenticated as well as encrypted. *See also* server certificate.

**CA vault.** A vault created automatically for each CA that is used when processing encrypted requests, including requests to create vaults or issue certificates.

**CAST-64.** A block cipher algorithm that uses a 64-bit block size and a 6-bit key. It was designed by Carlisle Adams and Stafford Tavares.

**CCA.** IBM Common Cryptographic Architecture.

**certificate.** *See* digital certificate.

**certificate management system (CMS).** Software that manages digital certificates and maintains information about certificates and CRLs in the Directory. A CMS system provides services such as issuing, revoking, suspending, resuming, and renewing rights to the use of digital certificates. *See also* Vault Certificate Management System

**certificate revocation list (CRL).** A digitally signed, time-stamped list of certificates that have been revoked by the certificate authority. The certificates in this list should be considered unacceptable. *See also* digital certificate.

**certificate authority (CA).** The entity, software application, or persons responsible for following an organization's security policies and assigning secure electronic identities in the form of certificates. The CA processes requests to issue, renew, and revoke certificates. In Vault Registry, the CA also authorizes RAs to approve requests to issue certificates. *See also* digital certificate.

**CGI.** Common Gateway Interface.

**chain validation.** The validation of all CA signatures in the trust hierarchy through which a given certificate was issued. For example, if a CA was issued its signing certificate from another CA, both signatures will be validated as part of validating the certificate presented by the user.

**class.** In object-oriented design or programming, a group of objects that share a common definition and therefore share common properties, operations, and behavior.

**cleartext.** Data that is not encrypted.

**client.** (1) A functional unit that receives shared services from a server. (2) A computer or program that requests a service of another computer or program.

**client/server.** A model in distributed processing in which a program at one site sends a request to a program at another site and waits for a response. The requesting program is called a client; the answering one is called a server.

**CMS.** Certificate management system.

**Common Cryptographic Architecture (CCA).** IBM software that enables a consistent approach to cryptography on major IBM computing platforms. It supports application software written in a variety of programming languages. Application software can call on CCA services to perform a broad range of cryptographic functions, including DES and RSA encryption.

**Common Gateway Interface (CGI).** Standard method of transmitting information between Web pages and Web servers.

**confidentiality.** The property of not being divulged to unauthorized parties.

**configuration manager.** Vault Registry software that loads configuration files and manages their content. The information in each configuration file may be divided into blocks with the block name enclosed in square brackets. Within each block, a set of `attribute=value` entries is defined. When a configuration file is loaded, the configuration manager provides a handle that is used to retrieve the value of any defined attribute.

**context.** *See* security context.

**context ID.** A unique integer assigned when the security context for a vault user is created.

**credential.** Confidential information used to prove one's identity in an authentication exchange. In network computing environments, the most common type of credential is a certificate that has been created and signed by a CA.

**CRL.** Certificate revocation list.

**cross-certification.** A trust model in which CAs that trust each other sign the certificates of the other's users.

**cryptographic.** Pertaining to the transformation of data to conceal its meaning.

**cryptography.** In computer security, the principles, means, and methods for encrypting plaintext and decrypting encrypted text.

# D

**daemon.** A program that carries out tasks in the background. It is implicitly invoked when a condition occurs that requires its help. A user need not be aware of a daemon because it is usually automatically spawned by the system. A daemon may live forever or be regenerated at intervals.

The term (pronounced *demon*) comes from mythology. Later, it was rationalized as the acronym DAEMON: Disk And Execution MONitor.

**Data Encryption Standard (DES).** An encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard. It was originally developed at IBM. DES has been extensively studied since its publication and is a well-known and widely used cryptosystem.

DES is a symmetric cryptosystem. When it is used for communication, both the sender and receiver must know the same secret key. This key is used to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. DES has a 64-bit block size and uses a 56-bit key during encryption. It is was originally designed for implementation in hardware. NIST has recertified DES as an official U.S. government encryption standard every five years.

**decipher.** To decrypt.

**decrypt.** To undo the encryption process.

**DEK.** Document encrypting key.

**DES.** Data Encryption Standard.

**dialog box.** A task panel element in a graphical user interface. It contains action buttons and various options that allow a user or administrator to complete a particular task.

**Diffie-Hellman.** A method of establishing a shared key over an insecure medium, named after the inventors (Diffie and Hellman).

**digital certificate.** An electronic credential issued by a trusted third party to a person or entity. Each certificate is signed with the private key of the CA. It vouches for an individual, business, or organizational identity. In Vault Registry, it can be one of four types: vault, organization, signing, and encryption.

Depending on the role of the CA, the certificate can attest to the authority of the bearer to conduct e-business over the Internet. In a sense, a digital certificate performs a similar role to a driver's license or a medical diploma. It certifies that the bearer of the corresponding private key is authorized to conduct certain e-business activities.

A certificate contains information about the entity it certifies, whether person, machine, or computer program. It includes the certified public key of that entity.

**digital certification.** The process during which a trusted third party issues an electronic credential that vouches for an individual, business, or organizational identity.

**digital signature.** A coded message added to a document or data that guarantees the identity of the sender.

A digital signature can provide a greater level of security than a physical signature. The reason for this is that a digital signature is not an encrypted name or series of simple identification codes. Instead, it is an encrypted summary of the message that is being signed. Thus, affixing a digital signature to a message provides solid identification of the sender. (Only the sender's key can create the signature.) It also fixes the content of the message that is being signed (the encrypted message summary must match the message content or the signature is invalid). Thus, a digital signature cannot be copied from one message and applied to another as the summary, or hash, would not match. Any alterations to the message, after it is signed, would also invalidate the signature.

**Digital Signature Algorithm (DSA ).** A public key algorithm that is used as part of the Digital Signature Standard. It cannot be used for encryption, only for digital signatures.

**direct enrollment.** An enrollment mechanism available in the Vault Registration Application that enables users to apply for organization certificates without first obtaining a vault. This approach is useful for applications that need to be protected by a secure Web server, but do not require the security of a vault. *Contrast with* vault-based enrollment.

**Directory.** A hierarchical structure intended as a global repository for information relating to communications (such as e-mail, cryptographic exchanges, or telephone). The Directory stores specific items that are essential to the PKI structure, including:

- Public keys and public key certificates
- Certificate revocation lists
- Disclosure statements with respect to CAs and repositories
- Access guidelines, policies, and fees

The Directory is physically distributed across multiple systems with different organizations or countries owning and managing different parts. The overall structure under which these parts fit together is the namespace.

Data in the Directory is organized hierarchically in the form of a tree, with the top of the tree being the root. No entries are allowed in the root directory. Often, higher level organizations represent individual countries, governments, or companies. Users and devices are typically represented as leaves of each tree. These users, organizations, localities, countries, and devices each have their own entry in the Directory Information Tree (DIT). Each entry in the tree consists of a number of typed attributes that provide information about the object represented by the entry.

Each user entry in the Directory is bound with an associated distinguished name (DN). These are created as unique names when an attribute that is known to be unique to the real world object is included. For example:

```
c=US,o=IBM,ou=VaultReg,cn=CA1
```

**Directory entry.** The basic data item stored in the Directory. Each entry has a unique name, the distinguished name, and represents a physical entity that may belong to one or more object classes.

**dispatcher.** Vault Registry software that handles browser requests coming from the Service Supervisors. The dispatcher also handles requests coming from other vault processes, or from vault process threads that are sent through the Secure Depositor queue.

**distinguished name (DN).** The unique name of a data entry stored in the Directory. The DN uniquely identifies the position of an entry in the hierarchical structure of the Directory.

**DN.** Distinguished name.

**document encrypting key (DEK).** Typically, a symmetric encryption / decryption key, such as DES.

**domain.** *See* security domain.

**DSA.** Digital Signature Algorithm.

# E

**e-business.** The conducting of business transactions over networks and through computers. It includes buying and selling goods and services. It also includes transferring funds through digital communications.

**e-commerce.** Conducting business-to-business transactions. It includes buying and selling goods and services (with customers, suppliers, vendors, and others) on the Internet. It is a primary element of e-business.

**encipher.** To encrypt.

**encrypt.** To scramble information so that only someone knowing the appropriate decryption code can obtain the original information through decryption.

**encryption certificate.** In Vault Registry, a digital certificate that is used in the vault for certifying the encryption key used in the vault.

**encryption/decryption.** Using the public key of the intended recipient to encipher data for that person, who then uses the private key of the pair to decipher the data.

**enrollment attribute.** An enrollment variable that is contained within an application enrollment form and whose value reflects the information captured during the enrollment. The value of the enrollment attribute remains the same throughout the lifetime of the application.

**enrollment variable.** *See* enrollment attribute.

**entry.** *See* Directory entry.

**external structure.** *See* namespace.

**extranet.** A derivative of the Internet that uses similar technology. Companies are beginning to apply Web publishing, electronic commerce, messaging, and groupware to multiple communities of customers, partners, and internal staff.

## F

**File Transfer Protocol (FTP).** An Internet client/server protocol that can be used to transfer files between computers.

**firewall.** A gateway between networks that restricts the flow of information between networks. It is typically used to protect internal networks from unauthorized use from the outside.

**FTP.** File Transfer Protocol.

## G

**gateway.** A system that allows incompatible networks or applications to communicate with each other.

## H

**handle.** In the AIX operating system, a data structure that is a temporary local identifier for an object. Allocating a handle creates it. Binding a handle makes it identify an object at a specific location.

**handshake.** In a client/server connection, the establishment of communication protocols that will control the exchange of information during the life of the session.

**hash.** A mathematical summary, or one-way function, that is easy to generate and hard to revert. It acts as a fingerprint of a message. The message contents cannot be changed without altering the hash code.

**heartbeat file.** File used by the Vault Registry auto-restart monitor utility to store the information needed to monitor and restart processes.

**HTML.** Hypertext Markup Language.

**HTTP.** Hypertext Transaction Protocol.

**HTTP daemon.** A persistent process that handles Web-based communications with browsers and other programs in a network.

**hypermedia.** An extension of hypertext to enable links to graphics, sound, video, and other kinds of resources.

**hypertext.** Text that contains words, phrases, or graphics that the reader can click with the mouse to retrieve and display another document. These words, phrases, or graphics are known as hyperlinks. Retrieving them is known as linking to them.

**hypertext link.** A connection between one piece of electronic information and another.

**Hypertext Markup Language (HTML).** A markup language for coding Web pages. It is based on SGML.

**Hypertext Transaction Protocol (HTTP).** An Internet client/server protocol for transferring hypertext files across the Web.

## I

**IETF (Internet Engineering Task Force).** A group that focuses on engineering and developing protocols for the Internet. It represents an international community of network designers, operators, vendors, and researchers. The IETF is concerned with the development of the Internet architecture and the smooth use of the Internet.

**instance.** In DB2, an instance is a logical database management environment for storing data and running applications. It allows a common set of configuration parameters to be defined for multiple databases. In the Vault Registration Application, an application domain can use a unique database, share a database with other domains, or share an instance with multiple databases.

**integrity.** A system protects the integrity of data if it prevents unauthorized modification (as opposed to protecting the confidentiality of data, which prevents unauthorized disclosure).

**internal structure.** *See* schema.

**International Standards Organization (ISO).** An international organization tasked with developing and publishing standards for everything from wine glasses to computer network protocols.

**International Telecommunication Union (ITU).** An international organization within which governments and the private sector coordinate global telecom networks and services. It is the leading publisher of telecommunication technology, regulatory and standards information.

**Internet.** A world-wide collection of networks that provide electronic connection between computers. It enables them to communicate with each other via software devices such as electronic mail or Web browsers such as Netscape Navigator. For example, some universities are on a network that in turn links with other similar networks to form the Internet.

**intranet.** A network within an enterprise that usually resides behind firewalls. It is a derivative of the Internet that uses similar technology. Technically, intranet is a mere extension of the Internet. HTML (the language used for graphical representation of information) and HTTP (the protocol that moves hypertext files across the Internet) are some of the commonalties.

**IPSec.** An Internet Protocol Security standard developed by the IETF. IPSec is a network layer protocol designed to provide cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality. Because of its strong authentication features, it has been adopted by many VPN product vendors as the protocol for establishing secure point-to-point connections through the Internet.

**ISO.** International Standards Organization.

**ITU.** International Telecommunication Union.

## J

**Java.** A set of network-aware, non-platform-specific computer technologies developed by Sun Microsystems, Incorporated. The Java environment consists of the Java OS, the virtual machines for various platforms, the object-oriented Java programming language, and several class libraries.

**Java applet.** *See* applet. *Contrast with* Java application.

**Java application.** A stand-alone program written in the Java language that runs outside the context of a Web browser.

**Java class.** A unit of Java program code.

**Java language.** A programming language, developed by Sun Microsystems, designed specifically for use in applet and agent applications.

**Java OS.** A basic, small-footprint operating system that supports Java.

## K

**key.** A quantity used in cryptography to encipher or decipher information.

**key file.** A file that contains the public keys of the user who owns it. In Vault Agent applications, the key file can be exported by one vault owner and imported by another, allowing the two to exchange secure, encrypted messages. The key files of the vaults with which you want to communicate must be stored in your personal address book.

**key pair.** Corresponding keys used in asymmetric cryptography. One key is used to encrypt and the other to decrypt.

## L

**LDAP.** Lightweight Directory Access Protocol.

**Lightweight Directory Access Protocol (LDAP ).** A protocol used to access the Directory.

**Lotus Domino Go Webserver.** The underlying Web server platform for the Vault Controller and the Vault Registration Application. It is a secure, scalable, high-performance, transaction-ready Web server.

## M

**Management Information Base (MIB).** Defines the schema used to create an SNMP trap.

**Master RA.** A primary Vault Registration Application component that manages registration and certification requests. It is composed of background (daemon) processes that:

- Receive messages from the enrollment facilities
- Update the application databases
- Call policy exits
- Generate certificates
- Generate e-mail notifications

One or more Master RAs can run simultaneously; the actual number in operation is largely determined by scalability and the security considerations of the organization. Any Master RA can be configured to support one or more application domains.

**Master RA user.** A user who approves and administers requests from users who enroll as RAs or Vault Registry operators. Using the RA Desktop, a Master RA user can process applications from RAs, process applications from operators, and revoke, suspend, and resume vaults owned by RAs and operators.

**MD2.** A 128-bit message digest hash function designed by Ron Rivest. It is used along with MD5 in the PEM protocols.

**MD4.** A 128-bit message digest hash function designed by Ron Rivest. It is several times faster than MD2.

**MD5.** A one-way message digest hash function (designed by Ron Rivest) that is an improved version of MD4. MD5 processes input text in 512-bit blocks, divided into 16 32-bit sub-blocks. The output of the algorithm is a set of four 32-bit blocks, which concatenate to form a single 128-bit hash value. It is also used along with MD2 in the PEM protocols.

**message digest.** An irreversible function that takes an arbitrary-sized message and outputs a fixed length quantity. MD5 is an example of a message digest algorithm.

**MIB.** Management Information Base.

**MIME (Multipurpose Internet Mail Extensions).** A freely available set of specifications that allows the interchange of text in languages with different character sets. it also allows multimedia e-mail among many different computer systems that use Internet mail standards. For example, the e-mail messages may contain character sets other than US-ASCII, enriched text, images, and sounds.

**modulus.** In the RSA public key cryptosystem, the product (n) of two large primes: p and q. The best size for an RSA modulus depends on one's security needs. The larger the modulus, the greater the security. The current RSA Laboratories–recommended key sizes are based on the planned use for the key: 768 bits for personal use, 1024 bits for corporate use, and 2048 bits for extremely valuable keys like the key pair of a CA. A 768-bit key is expected to be secure until at least the year 2004.

## N

**namespace.** As relates to the Directory, the external structure of names that is accessible to users. *Contrast with* schema.

**National Language Support (NLS).** Support within a product for differences in locales, including language, currency, date and time format, and numeric presentation.

**National Security Agency (NSA).** The official security body of the U.S. government.

**Net.** Slang for the Internet.

**NIST.** National Institute of Standards and Technology, formerly known as NBS (National Bureau of Standards). It promotes open standards and interoperability in computer-based industries.

**NLS.** National language support.

**nonce.** A string that is sent down from a server or application requesting user authorization. The user being asked for authentication signs the nonce with a private key. The user's public key and the signed nonce are sent back to the server or application that requested authentication. The server then attempts to decipher the signed nonce with the user's public key. If the deciphered nonce is the same as the original nonce that was sent, the user is authenticated.

**non-repudiation.** The use of a digital private key to prevent the signer of a document from falsely denying having signed it.

**non-vault-based enrollment.** *See* direct enrollment.

**NSA.** National Security Agency.

## O

**object.** In object-oriented design or programming, an abstraction encapsulating data and the operations associated with that data. *See also* class.

**object type.** The kind of object that can be stored in the Directory. For example, an organization, meeting room, device, person, program, or process.

**ODBC.** Open Database Connectivity.

**Open Database Connectivity (ODBC).** A standard for accessing different database systems.

**Open Systems Interconnect (OSI).** The name of the computer networking standards approved by ISO.

**Operations Center.** An extension of the Vault Registration Application that provides authorized Vault Registry operators with a graphical interface for performing system operations and administrative tasks.

**operator.** In Vault Registry, an administrative role that allows users to execute tasks through the Operations Center. An operator must be apply for a certificate that allows access to the Operations Center; the Master RA user can approve or reject the application.

**organization certificate.** A digital certificate that allows its possessor secure access to organization applications. It is generated from a CA and approved by an RA belonging to the organization. That is, the organization controls the issuance, security policy, and revocation of these certificates.

The organization certificate can be used in different ways depending on the location of the secure applications:

- When secure applications are located on a Web server hosted by the organization, the organization certificate is used to authenticate the Web server using SSL. Without this certificate, access to the Web server is denied.
- When secure applications are located on a Vault Controller, the organization certificate can be used to access a secure application running in a user's vault. Without this certificate, access to the application is denied.

**OSI.** Open Systems Interconnect.

# P

**PAB.** Personal address book.

**PC card.** Similar to a smart card, and sometimes called a PCMCIA card. This card is somewhat larger than a smart card and usually has a greater capacity.

**PEM.** Privacy-Enhanced Mail.

**permission slip.** A non-RA user can issue a service request to the CA Agent if, and only if, an RA registers the requested action with the CA. An RA uses a permission slip to perform this preapproval registration. The permission slip gives the non-RA user written consent to access the CA Agent daemon to run a command. It contains the enciphered and signed DN of the user who is allowed to run the command. It also specifies the number of days the permission slip is valid.

**personal address book (PAB).** A structure that stores key files exported from one vault user to another. When an application is initialized with SSL, the Secure Depositor can obtain the a key file from the user's PAB. Doing so enables the user to exchange secure, encrypted messages with the vault owned by the owner of that key file.

**PKCS.** Public Key Cryptography Standards.

**PKCS #1.** *See* Public Key Cryptography Standards.

**PKCS #7.** *See* Public Key Cryptography Standards.

**PKCS #10.** *See* Public Key Cryptography Standards.

**PKI.** Public key infrastructure.

**plaintext.** (1) Unencrypted data. *Synonymous with* cleartext. (2) *Synonym for* clear data.

**policy exit.** In the Vault Registration Application, a customer-defined program that is called by the end-user and RA support daemons. The rules specified in each policy exit allow the organization's security preferences to be applied to the enrollment process on an application domain-specific basis. The policy exits can obtain information they need to complete a task from the RA database. Because all policy exit actions are logged in the RA database, an RA can use the RA Desktop to review its action history.

**privacy.** Protection from the unauthorized disclosure of data.

**Privacy-Enhanced Mail (PEM).** The Internet Privacy-Enhanced Mail standard, adopted by the Internet Architect Board (IAB) to provide secure electronic mail over the Internet. The PEM protocols provide for encryption, authentication, message integrity, and key management.

**private key.** The key in a public/private key pair that is available only to its owner. It enables the owner to receive a private transaction or make a digital signature. *Synonymous with* secret key. Data signed with a private key can be verified only with the corresponding public key. *Contrast with* public key. *See also* public/private key pair.

**protocol.** An agreed upon convention for inter-computer communication.

**proxy server.** An intermediary between the computer requesting access (A) and the computer being accessed (B). Thus, if an end user makes a request for a resource from computer A, this request is directed to a proxy server. The proxy server makes the request, gets the response from computer B, and then forwards the response to the end user. Proxy servers are useful for accessing World Wide Web resources from inside a firewall.

**public key.** The key in a public/private key pair that is made available to others. It enables them to direct a transaction to the owner of the key or verify a digital signature. Data encrypted with the public key can be decrypted only with the corresponding private key. *Contrast with* private key. *See also* public/private key pair.

**Public Key Cryptography Standards (PKCS).** Informal inter-vendor standards developed in 1991 by RSA Laboratories with representatives from various computer vendors. These standards cover RSA encryption, the Diffie-Hellman agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax, and certification syntax.

- PKCS #1 describes a method for encrypting data using the RSA public key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes.
- PKCS #7 specifies a general format for cryptographic messages.
- PKCS #10 describes a standard syntax for certification requests.

**public key infrastructure (PKI).** A standard for security software based on public key cryptography. The PKI is a system of digital certificates, certificate authorities, registration authorities, certificate management services, and distributed directory services. It is used to verify the identity and authority of each party involved in any transaction over the Internet. These transactions might involve operations where identity verification is required. For example, they might confirm the origin of proposal bids, authors of e-mail messages, or financial transactions.

The PKI achieves this by making the public encryption keys and certificates of users available for authentication by a valid individual or organization. It provides online directories that contain the public encryption keys and certificates that are used in verifying digital certificates, credentials, and digital signatures.

The PKI provides a means for swift and efficient responses to verification queries and requests for public encryption keys. It also identifies potential security threats to the system and maintains resources to deal with security breaches. Lastly, the PKI provides a digital timestamping service for important business transactions.

**public/private key pair.** A public/private key pair is part of the concept of key pair cryptography (introduced in 1976 by Diffie and Hellman to solve the key management problem). In their concept, each person obtains a pair of keys, one called the public key and the other called the private key. Each person's public key is made public while the private key is kept secret. The sender and receiver do not need to share secret information: all communications involve only public keys, and no private key is ever transmitted or shared. It is no longer necessary to trust some communications channel to be secure against eavesdropping or betrayal. The only requirement is that public keys are associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by using public information. However, the message can be decrypted only with a private key, which is in the sole possession of the intended recipient. Furthermore, key pair cryptography can be used not only for privacy (encryption), but also for authentication (digital signatures).

# R

**RA.** Registration authority.

**RA Desktop.** A Java applet that provides RAs with a graphical interface for processing end-user requests for certificates and vaults. When accessed by a Master RA user, the Desktop's title bar indicates that fact. It allows the Master RA user to process only those requests that originate from an RA or operator.

**RC2.** RC2 is a variable key-size block cipher designed by Ron Rivest for RSA Data Security. RC stands for Ron's Code or Rivest's Cipher. It is faster than DES and is designed as a drop-in replacement for DES. It can be made more secure or less secure than DES against exhaustive key search by using appropriate key sizes. It has a block size of 64 bits and is about two to three times faster than DES in software. RC2 can be used in the same modes as DES.

An agreement between the Software Publishers Association (SPA) and the United States government gives RC2 special status. This makes the export approval process simpler and quicker than the usual cryptographic export process. However, to qualify for quick export approval a product must limit the RC2 key size to 40 bits with some exceptions. An additional string can be used to thwart attackers who try to precompute a large look-up table of possible encryptions.

**Recovery Agent.** An extension of the Vault Registration Application that enables users with the appropriate privileges to support recovery and synchronization of the system. Users must have privileges for executing reconciliation between Vault Registration Application databases and Vault Registry repositories.

**RefID.** A reference ID that is used along with an authorization code to access an Entrust-ready VPN product. Users enroll and apply for a RefID and Authcode pair through the Vault Registration Application.

**Registration Authority (RA).** An entity (person or process) authorized to administer applications for digital certificates. An RA can approve, reject, and revoke certificates. Each RA can administer applications for one or more application domains.

**registration process.** The steps that take place to validate a user so that the user and the user's public key can become certified and participate in transactions. This process can be local or Web-based, automated or administered by a human registration authority.

**repository.** An organized data store, providing storage and access to content. In Vault Registry, separate repositories exist for the Directory, each CA, each Vault Controller vault, and each Vault Registration Application domain. *See also* target.

**repository state.** In Vault Registry, the status of an entry in one of its repositories (Directory database, CA database, or Vault Controller vault). In the Vault Registration Application, the repository state corresponds to the application state; each application state tracked in a Vault Registration Application database has a corresponding repository state in a Vault Registry repository.

**repudiation.** To reject as untrue; for example, to deny that you sent a specific message or submitted a specific request.

**retrieval filter.** The search criteria the RA Desktop processes use.

**RFC 1424.** One of the specification documents for PEM (Part IV: Key Certification and Related Services). It describes three types of service in support of PEM: key certification, certificate revocation list (CRL) storage, and CRL retrieval.

**RSA.** A public key cryptographic algorithm named for its inventors (Rivest, Shamir, and Adelman) that is used for encryption and digital signatures.

## S

**schema.** As relates to the Directory, the internal structure that defines the relationships between different object types. *Contrast with* namespace.

**Secure Depositor.** Vault Registry software that provides secure communication between vault processes by intervening in vault-to-vault communications. In other words, messages are sent from a vault process to a specific vault rather than directly to another vault process. The Secure Depositor library handles such functions as the following:

- Mapping distinguished names
- Encrypting and decrypting messages
- Validating messages

**Secure Depositor daemon.** A simple process that receives encrypted messages on a communication port and delivers the message to an appropriate queue.

**Secure Electronic Transaction (SET ).** An industry standard that facilitates secure credit card or debit card payment over untrusted networks. It incorporates authentication of cardholders, merchants, and card-issuing banks by issuing certificates.

**Secure Sockets Layer (SSL ).** An IETF standard communications protocol with built-in security services that are as transparent as possible to the end user. It provides a digitally secure communications channel.

An SSL-capable server usually accepts SSL connection requests on a different port than the standard HTTP requests. SSL creates a session during which the handshake needs to happen only once. After the handshake is finished, communication is encrypted. Message integrity checks are performed until the SSL session expires.

**security context.** In IBM Vault Registry, an opaque object, identified by a unique context ID. It contains security-related data pertaining to a single, thread-safe application instance. It is used to preserve the state of the application as it runs in the vault. It allows the user to resume the vault process from the point where the user last left it (for example, if the user closed the browser connection).

**security domain.** A group (a company, work group or team, educational or governmental) whose certificates have been certified by the same CA. Users possessing certificates signed by a CA can trust the identity of another user bearing a certificate signed by the same CA.

**server.** (1) In a network, a data station that provides facilities to other stations; for example, a file server. (2) In TCP/IP, a system in a network that handles the requests of a system at another site, called a client/server.

**server certificate.** A digital certificate issued by a CA that enables a Web server to conduct SSL-based transactions. When a browser connects to the server using the SSL protocol, the server sends the browser its public key. This enables the identity of the server to be authenticated. It also enables information sent to the server to be encrypted. In a Vault Registry system, server certificates are obtained through the Vault Registration Application. *See also* CA site certificate, digital certificate, and browser certificate.

**SET.** Secure Electronic Transaction.

**SGML.** Standard Generalized Markup Language.

**SHA-1 (Secure Hash Algorithm).** An algorithm designed by NIST and NSA for use with the Digital Signature Standard. The standard is the Secure Hash Standard; SHA is the algorithm used in the standard. SHA produces a 160-bit hash.

**sign.** To use your private key to generate a signature as a means of proving that you are responsible for and approve of the message being signed.

**signature certificate.** A digital certificate that is used in a vault for certifying the personal key used in the vault.

**signing/verifying.** Signing entails using a private digital key to sign a document. Verifying entails using the corresponding public key to verify the signature.

**Simple Mail Transfer Protocol (SMTP).** A protocol that transfers electronic mail over the Internet.

**Simple Network Management Protocol (SNMP).** A UNIX networking protocol used to obtain information from and issue instructions to other devices and systems.

Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications that monitor and control network elements. Network elements are devices such as hosts, gateways, and terminal servers, that have management agents responsible for performing the network management functions requested by the network management stations. SNMP is used to communicate management information between the network management stations and the agents in the network elements.

**site certificate.** *See* CA site certificate.

**smart card.** A piece of hardware, typically the size of a credit card, that can be used to store a user’s digital keys. A smart card can be password-protected.

**S/MIME.** A standard that supports the signing and encryption of e-mail transmitted across the Internet. *See* MIME.

**SMTP.** Simple Mail Transfer Protocol.

**SNMP.** Simple Network Management Protocol.

**SNMP trap.** An error condition in SNMP.

**SSL.** Secure Sockets Layer.

**standard.** A definition or format approved by a recognized standards organization or accepted as a de facto standard by the industry. Standards exist for communications protocols such as SSL.

**Standard Generalized Markup Language (SGML).** A standard for describing markup languages. HTML is based on SGML.

**supervisor.** A Vault Registry shared library that runs as part of the HTTP daemon. It acts as a link between the end user sitting at a browser and the application being run.

**symmetric cryptography.** Cryptography that uses the same key for both encryption and decryption. Its security rests in the key — revealing that the key means that anyone could encipher and decipher messages. The communication remains secret only as long as the key remains secret. *Contrast with* asymmetric key cryptography.

**symmetric key.** A key that can be used for both encryption and decryption. *Contrast with* asymmetric cryptography.

**System Management daemon.** An application that receives system and application events from every Vault Registry component. It processes each event according to its configuration. It places the event into a log file or sends notification of the event to a system management station.

## T

**target.** A designated or selected data source. *See also* repository.

**TCP/IP.** Transmission Control Protocol/Internet Protocol.

**Transmission Control Protocol/Internet Protocol (TCP/IP ).** A set of communication protocols that support peer-to-peer connectivity functions for local and wide area networks.

**triple DES.** A symmetric algorithm that encrypts the plaintext three times. Although a variety of ways exists to do this, the most secure form of multiple encryption is triple-DES with three distinct keys.

**trust domain.** A set of end user entities whose certificates have been certified by the same CA.

**trust model.** A structuring convention that governs how certificate authorities certify other certificate authorities.

**tunnel.** In VPN technology, an on-demand virtual point-to-point connection made through the Internet. Once connected, remote users can use the tunnel to exchange secure, encrypted, and encapsulated information with servers on the corporate private network.

**type.** *See* object type.

## U

**Uniform Resource Locator (URL).** A scheme for addressing resources on the Internet. The URL specifies the protocol, host name or IP address, port number, path, and resource details needed to access a resource from a particular machine.

**Unsolicited Vault Launch (UVL).** The Vault Registry feature that allows vaults to perform decryption of encrypted documents without the document owner's participation in the transaction if the requestor is on the document ACL.

**URL.** Uniform Resource Locator.

**user authentication.** The process of validating that the originator of a message is the identifiable and legitimate owner of the message. It also validates that you are communicating with the end user or system you expected to.

**user ID.** Unique identifier that refers to a person accessing the system.

**UVL.** Unsolicited Vault Launch.

## V

**validator vault.** A vault associated with one or more application domains that processes registration requests from users who do not yet have vault access certificates. For example, the validator vault allows users to connect to the Vault Controller to apply for a vault or renew an expiring certificate.

**vault.** In Vault Registry, a vault uses encryption to protect information against disclosure to unauthorized persons (such as system administrators and other vault owners). It also uses digital signing to protect against tampering, and digital certification to protect against communication with unknown parties. It also uses encryption, signing, and certification to transmit information securely to other vaults.

It is a storage area, owned by a particular UNIX account, that is linked to a user with a specific vault access certificate. The content of the vault is encrypted and contains an encryption key pair and signing key pair, both of which are password-protected. Each vault has a unique distinguished name (DN) in the Directory with a common name based on a unique vault ID. There is a unique mapping between the vault ID (which identifies the user account and the user's home directory) and the vault access certificate. *See also* CA vault and validator vault.

**vault access certificate.** A digital certificate that enables a user to access a vault process. It can be stored in a Web browser. It is used to authenticate the user when establishing an SSL connection between a Web browser and the Vault Controller.

**Vault Agent.** A Vault Registry client component that allows an organization to run applications outside the execution environment of the Vault Controller. A Vault Agent vault can exchange secure messages with vaults managed by the Vault Controller or another Vault Agent application.

**vault-based enrollment.** An enrollment mechanism available in the Vault Registration Application that enables users to apply for a vault access certificate and obtain a vault before obtaining an organization certificate. *Contrast with* direct enrollment.

**Vault CA.** The Vault Controller CA that issues vault access certificates.

**Vault Certificate Management System (Vault CMS).** The underlying certificate management system for Vault Registry applications. To comply with U.S. Government export regulations, a version specific to an encryption level is included in the product distribution package. *See also* certificate management system.

**Vault Certificate Validator.** A Vault Registry client component that allows an organization to develop custom applications for validating certificates. A user's certificate can be validated by examining local certificate management databases or entries in the Directory.

**Vault Controller.** A major Vault Registry component, it provides and manages secure execution environments for server programs running on behalf of individuals who have used public key credentials to identify themselves. Separate and persistently unique execution environments and resources, known as vaults, are dedicated to each authorized user. A vault is accessible from any SSL-enabled Web browser that contains the corresponding vault access certificate.

The Vault Controller uses encryption to protect information stored in vaults from disclosure to unauthorized persons (for example, system administrators and other vault users). It also uses digital signatures to protect vaults from malicious tampering, and digital certification to protect vaults from untrusted communication with unknown parties.

Information can be transmitted securely between vaults by using encryption, signatures, and certificates. All vaults managed by an instance of the Vault Controller use a single instance of Vault CMS to handle encryption, digital signing, and certificate management.

**vault daemon.** A persistent process that accepts requests from the supervisor to start vault processes. It also launches the HTTP daemon at system startup.

**vault process.** A program that runs in a vault on behalf of an end user.

**Vault Registration Application.** A Vault Registry application that provides digital registration services. Features include the ability to use a Web interface to handle requests, obtain certificates (with or without vaults), and implement custom security policy controls. Extensive RA support is provided for approving, revoking, and renewing certificates. It also includes support for multiple RAs, and manual and automated approval processes.

**Vault Registry.** An IBM software product that provides a secure, Web-based, public/private key pair framework that enables organizations to run e-commerce applications in dedicated, highly-trusted execution environments. It uses certificates to authenticate the parties involved in an e-commerce transaction. It also uses key pair cryptography to protect the confidentiality and integrity of each transaction.

**VC Agent.** Vault Controller Agent. A daemon process that runs in a vault, controls access to privileged vault operations, and is used only for recovery actions.

**VPN.** Virtual Private Network.

**Virtual Private Network (VPN).** A private data network that uses the Internet rather than phone lines to establish remote connections. Because users access corporate network resources through an Internet Service Provider (ISP) rather than a telephone company, organizations can significantly reduce remote access costs. A VPN also enhances the security of data exchanges. In traditional firewall technology, message content can be encrypted, but the source and destination addresses are not. In VPN technology, users can establish a tunnel connection in which the entire information packet (content and header) is encrypted and encapsulated. VPN support is a separately orderable feature of IBM Vault Registry. If installed, users can use the Vault Registration Application to obtain the credentials they need to access VPN products, including the Entrust IDs required for Entrust applications.

**VRA Database.** Contains information about the certificate applications for one or more application domains. The database stores enrollment data and keeps track of all changes to a certificate application throughout its life cycle. The database can be updated by policy exits or by administrators using the RA Desktop.

## W

**Web.** Slang for the World Wide Web.

**Web browser.** Client software that runs on your desktop PC and enables you to browse the World Wide Web or local HTML pages. It is a retrieval tool that provides universal access to the large collection of hypermedia material available in the Web and Internet. Some browsers can display text and graphics while some can display only text. Most browsers can handle the major forms of Internet communication, such as FTP transactions. Examples are Netscape Navigator and Microsoft Internet Explorer.

**Web server.** A server program that responds to requests for information resources from browser programs. *See also* server.

**World Wide Web (WWW).** That part of the Internet where a network of connections is established between computers containing hypermedia materials. These materials provide information and can provide links to other materials in the WWW and Internet. WWW resources are accessed through a Web browser program.

## X

**X.500.** A standard for implementing a multipurpose distributed and replicated directory service by interconnecting computer systems. Jointly defined by the International Telecommunications Union (ITU), formerly known as CCITT, and the International Organization for Standardization and International Electro-Chemical Commission (ISO/IEC).

**X.509 certificate.** A widely-accepted certificate standard designed to support secure management and distribution of digitally signed PKI certificates across secure Internet networks. The X.509 certificate defines data structures that accommodate procedures related to distribution of public keys digitally signed by trusted third parties.

**X.509 Version 3 certificate.** The X.509v3 certificate has extended data structures for storing and retrieving certificate application information, certificate distribution information, certificate revocation information, policy information, and digital signatures.

X.509v3 processes create time-stamped CRLs for all certificates. Each time a certificate is used, X.509v3 capabilities allow the application to check the validity of certificate. It also allows the application to determine that the certificate is not on that CRL. X.509v3 CRLs can be constructed on the basis of a specific validity period. They can also be based on other circumstances that may cause a certificate to become invalid, such as when an employee terminates employment.

# Bibliography

This bibliography lists the publications in the IBM Vault Registry library and publications pertaining to related products that may assist you when installing, administering, or using a Vault Registry system.

The *IBM Vault Registry Documentation* CD-ROM contains softcopy versions of all the Vault Registry product publications, in all available languages. For information about viewing or printing these files, see the *Readme_xx* file on that CD-ROM, where *xx* represents one of the following possible language versions:

- *en*, for English
- *fr*, for French
- *de*, for German
- *ja*, for Japanese
- *zh*, for Traditional Chinese

## Vault Registry Library

- *IBM Vault Registry General Information Guide*, GH09-4516-02
- *IBM Vault Registry Installation and Configuration Guide*, SH09-4519-02
- *IBM Vault Registry System Operations Guide*, SH09-4518-02
- *IBM Vault Registry Messages and Codes*, SH09-4517-02
- *IBM Vault Controller for AIX Programming Guide*, SH09-4525-02
- *IBM Vault Controller for AIX Programming Reference*, SH09-4524-02
- *IBM Vault Registry Licensed Program Specifications*, GH09-4526-02

## Vault Registry Client Components Library

- *IBM Vault Agent User Guide and Reference*, SH09-4522-02
- *IBM Vault Certificate Validator User Guide and Reference*, SH09-4523-02
- *IBM Vault Agent License Information*, GH09-4540-00
- *IBM Vault Certificate Validator License Information*, GH09-4541-00

## Vault Registration Application Library

- *IBM Vault Registration Application for AIX Customization Guide*, SH09-4521-02
- *IBM Vault Registry Registration Authority User Guide*, SH09-4520-02

## Related Products Library

- *Lotus Domino Go Webserver Quick Beginnings* and *Webmaster's Guide*.

  To view these books, go to the Domino Go Webserver Web site at the following URL:

  `www.ics.raleigh.ibm.com/dominogowebserver`
- *IBM DSSeries LDAP Directory Programming Reference* (HTML file, available on the *Vault Registry Documentation* CD-ROM)
- *IBM DB2 Universal Database for UNIX, Quick Beginnings*, S10J-8148-00
- *IBM DB2 Universal Database Administration Guide*, S10J-8157-00
- *IBM DB2 Universal Database Command Reference*, S10J-8166-00
- *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program*, SCB1-8610-01
- *IBM Tivoli TME 10 NetView User's Guide for Beginners*, GC31-8439-00

# Index

Program Number:  5648–B28

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GH09-4516-02