Tivoli® SecureWay® Public Key Infrastructure

Up and Running

Version 3    Release 7.0

GC32-0472-02
Third Edition (November 2000)

This edition applies to IBM SecureWay Trust Authority, program 5648-D09, version 3 release 7 modification 0, and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1999, 2000. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

About this book ............................................................ vii
  Audience ................................................................... vii
  Conventions ................................................................ vii
  What’s new in this release ............................................ viii

Chapter 1. Understanding Trust Authority ................................. 1
  What is FirstSecure? ...................................................... 1
  What is Trust Authority? ................................................. 1
  Components ................................................................ 3
    Trust Authority server ................................................. 3
    Registration Authority .................................................. 3
    Certificate Authority ................................................... 6
    Audit subsystem .......................................................... 7
    Web server ................................................................ 7
    Database system ........................................................ 8
    Directory server ........................................................ 8
    4758 cryptographic coprocessor ....................................... 8
    Client application ....................................................... 9
  Key backup and recovery facility ........................................ 10
  Architecture .................................................................. 10
    Public key infrastructure ............................................ 10
    PKIX CMP protocol .................................................. 10
    LDAP protocol .......................................................... 11
    Object stores ........................................................... 11
    Smart card support ..................................................... 11
  Trust model .................................................................. 12
    Code signing ............................................................. 12
    Message signing ....................................................... 12
    Data encryption ........................................................ 12
    KeyStores ................................................................. 12
  Supported standards ...................................................... 12
    X.509 version 3 certificates .......................................... 13
  Related information ...................................................... 14
  Year 2000 readiness ...................................................... 15
  Service and support ...................................................... 15

Chapter 2. System requirements .......................................... 17

Public Key Infrastructure Up and Running
| Chapter 5. Installing Trust Authority on Windows NT | 49 |
| Setting up Windows NT | 50 |
| Installing the database software | 51 |
| Installing the Web server software | 52 |
| Install the JDK | 52 |
| Install IBM HTTP Server | 52 |
| Install WebSphere Application Server. | 53 |
| Set up IP aliases | 54 |
| Installing SecureWay Directory | 54 |
| Install Directory software | 54 |
| Use the Directory with Trust Authority | 54 |
| Confirm system settings. | 55 |
| Installing Trust Authority | 55 |
| Install the server software | 55 |
| Change bootstrap values | 57 |
| Run the post-installation configuration program | 58 |
| Post-installation checklist. | 59 |
| Run the backup utility | 60 |
| Upgrading the WebSphere Software | 60 |

| Chapter 6. Configuring Trust Authority | 63 |

| Chapter 7. Getting started | 65 |
| System administration | 65 |
| RA administration | 66 |
About this book

This book provides you with the information you need to become productive with an IBM® SecureWay® Trust Authority system. It discusses the following topics:

- How your organization can use Trust Authority to conduct encrypted, authenticated, and confidential transactions over the Internet. Using the Trust Authority registration facility, you can easily issue digital certificates to trusted parties and control whether or not a certificate is renewed or revoked.
- Guidelines to help you plan for Trust Authority, such as how to integrate Trust Authority components with other products installed at your site.
- Procedures for installing the product on an IBM AIX® platform or under Microsoft Windows NT.
- Pointers to other documents that can help you use the Trust Authority user interfaces and administration tools.

Audience

This book addresses a varied audience.

- If you are a marketing manager, this book shows you how to incorporate Trust Authority into your organization’s electronic business (e-business) strategy.
- If you are a security manager, this book shows you how to incorporate Trust Authority into your organization’s network security strategy.
- If you are a system administrator, this book assumes that you have experience with installing and configuring products in a network environment. You should be knowledgeable about the following concepts:
  - Hardware installation and configuration
  - Internet communications protocols, in particular TCP/IP and Secure Sockets Layer (SSL)
  - Web server administration
  - Public key infrastructure (PKI) technology, including Directory schemas, the X.509 version 3 standard, and the Lightweight Directory Access Protocol (LDAP)
  - Relational database systems, in particular IBM DB2® Universal Database

Conventions

This book uses the following typographic conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>User interface elements such as check boxes, buttons, and items inside list boxes.</td>
</tr>
<tr>
<td>monospace</td>
<td>Syntax and sample code.</td>
</tr>
<tr>
<td><strong>bold monospace</strong></td>
<td>Text that the user must type.</td>
</tr>
<tr>
<td>italic monospace</td>
<td>Variable values that the user must supply.</td>
</tr>
<tr>
<td>→</td>
<td>Shows a series of selections from a menu. For example: Select <strong>File → Run</strong> means click <strong>File</strong> and then click <strong>Run</strong>.</td>
</tr>
</tbody>
</table>
What’s new in this release

Trust Authority 3.7.0 consists of the following new features and functions:

- Key Backup and Recovery. This feature enables you to backup and recover the end entity certificates and their corresponding public and private keys certified by Trust Authority.

- Multiple RA Domains. This feature allows you to set up more than one Registration Authority (RA) under one Certificate Authority (CA). Each RA can be configured to have a different certificate issuing policy, allowing easier management and certificate approval control.

- Suspend and Resume Certificates. This feature allows you to temporarily suspend the authorization of a certificate and then resume the authorization at a later time. Before certificates had to be revoked and then reissued to achieve the same type of effect.

- Trust Chain Delivery. This feature enables an RA to deliver the entire trust chain of the CA that signs a certificate. This means that the authorization for a certificate can be traced back to the highest level of a hierarchy for a browser or server certificate. The delivery of the trust chain can be toggled on or off depending on your customer’s needs.

- Downward Hierarchy. Trust Authority 3.7.0 is now capable of granting a CA certificate to a Trust Authority CA or a third party CA, thus establishing a downward hierarchy.

Note: Trust Authority 3.7.0 only supports AIX. It does not support Windows NT for this release. Trust Authority 3.7.0 is being released in English only.
Understanding Trust Authority

This chapter provides an overview of IBM® SecureWay® Trust Authority. Following a discussion of the IBM® FirstSecure product family, it describes the Trust Authority components and how they interact.

To obtain more information about Trust Authority, and to stay aware of product enhancements, access the IBM SecureWay Trust Authority Web site:
http://www.tivoli.com/support/

What is FirstSecure?
FirstSecure is part of the IBM Integrated Security Solutions. FirstSecure is a comprehensive set of building blocks that help your company:

- Establish a secure e-business environment.
- Reduce the total cost of security ownership by simplifying security planning.
- Implement security policy more easily.
- Create a more effective and secure e-business environment.

FirstSecure includes virus protection, intrusion detection, access control, traffic content control, encryption, digital certification, firewall technology, and application development toolkits. These functions are delivered from IBM’s family of security products as well as through offerings from other companies, combining the best components of many security vendors. Trust Authority provides both encryption and digital certification functions.

Because FirstSecure is a collection of products that you can install independently, you can launch a planned move toward a secure environment. You can start in one area, test your improvements, and then continue to move toward more security. This approach reduces complexity and costs, and speeds deployment of Web applications and resources.

For information about FirstSecure and how Trust Authority interacts with and complements the other products in this security solution, see IBM SecureWay FirstSecure Planning and Integration. For more details, see the ITSO Redbook, "Understanding the IBM SecureWay FirstSecure Framework". To view this book, access the IBM Redbooks Web site:
http://www.ibm.com/redbooks

What is Trust Authority?
IBM SecureWay Trust Authority provides applications with the means to authenticate users and ensure trusted communications:
It allows organizations to issue, publish, and administer digital certificates in accordance with their registration and certification policies.

Support for Public Key Infrastructure for X.509 version 3 (PKIX) and Common Data Security Architecture (CDSA) cryptographic standards allows for vendor interoperability.

Digital signing and secure protocols provide the means to authenticate all parties in a transaction.

Browser- and client-based registration capabilities provide maximum flexibility.

Encrypted communications and secure storage of registration information help ensure confidentiality.

A Trust Authority system can run on IBM AIX/6000® (AIX®) and Microsoft® Windows NT® server platforms. It includes the following key features:

- A trusted Certificate Authority (CA) manages the life cycle of digital certification. To vouch for the authenticity of a certificate, the CA digitally signs each one it issues. It also signs certificate revocation lists (CRLs) to vouch for the fact that a certificate is no longer valid. To further protect its signing key, you can use cryptographic hardware, such as the IBM SecureWay 4758 PCI Cryptographic Coprocessor.

- A Registration Authority (RA) handles the administrative tasks behind user registration. The RA provides that only certificates that support your business activities are issued, and that they are issued only to authorized users. The administrative tasks can be handled through automated processes or human decision-making.

- A Web-based enrollment interface makes it easy to obtain certificates for browsers, servers, and other purposes, such as virtual private network (VPN) devices, smart cards, and secure e-mail.

- A Windows® application, the Trust Authority Client, enables end users to obtain and manage certificates without using a Web browser.

- A Web-based administration interface, the RA Desktop, enables authorized registrars to approve or reject enrollment requests and administer certificates after they have been issued.

- An Audit subsystem computes a message authentication code (MAC) for each audit record. If audit data is altered or deleted after it has been written to the audit database, the MAC enables you to detect the intrusion.

- Policy exits enable application developers to customize the registration processes.

- Integrated support for a cryptographic engine. To authenticate communications, the core Trust Authority components are signed with a factory-generated private key. Security objects, such as keys and MACs, are encrypted and stored in protected areas called KeyStores.


- Integrated support for IBM WebSphere™ Application Server and IBM HTTP Server. The Web server works with the RA server to encrypt messages, authenticate requests, and transfer certificates to the intended recipient.

- Integrated support for the award-winning IBM DB2® Universal Database.
Components

For illustrative purposes, the following diagram shows a Trust Authority system in which the server programs are distributed among three machines. In your organization, all three servers might co-exist on a single machine.

Trust Authority server
The Trust Authority server is the central server that ties the other components together. It maintains the configuration database and provides utilities for administering the system.

Registration Authority
The Registration Authority (RA) is the server component that manages the registration process. It enforces local business policies to provide that certificates are issued only to approved entities and used only for approved purposes. The primary tasks for an RA include:

- Confirming the identity of the requesting entity
- Verifying that the applicant is entitled to a certificate that contains the requested attributes and permissions
- Approving and rejecting requests to create, renew, or revoke certificates
- Verifying that an entity that attempts to access a secure application or resource holds the private key that is associated with the certificate’s public key

In Trust Authority, the registration facility installed on the RA server provides the framework to support a wide range of registration activities. When you configure the system, you
establish a registration domain that governs the business policies, certificate policies, and resources in accordance with your organization’s preferred registration and certification practices.

**Enrollment**

The RA provides support for a variety of enrollment protocols and certificate types. Enrollment features include:

- The use of a DB2® database to log encrypted registration and certificate data.
- Support for manual and automated registration approval processes.
- A collection of Java-based enrollment forms that allow users to request and obtain certificates through their own Web browsers. The enrollment process authenticates the client and server identities and delivers certificates to approved entities, with end-to-end encryption of all request data. It includes:
  - The delivery of certificates through the Secure Sockets Layer (SSL) for use with applications that are accessed from a Web browser or Web server.
  - The delivery of certificates through the PKIX Certificate Management Protocol (CMP) for use in a PKIX client application or to store on smart cards.
  - The delivery of certificates that support the Internet Protocol Security standard (IPSec) for use with secure VPN applications or IPSec-enabled devices.
  - The delivery of certificates that support Secure Multipurpose Internet Mail Extensions (S/MIME), for use with secure e-mail applications.
  - The delivery of notification letters that inform applicants about the approval or rejection of a request.
- A collection of certificate profiles that make it easy for users to obtain the type of certificate they need. The profiles define the intended purpose of the certificate and the certificate’s validity period. Based on information in the template, the RA is able to deliver a certificate in the proper format with the necessary certificate content.
  
  For information about the certificate types and certificate extensions supported by the RA, see “Supported standards” on page 13 and “X.509 version 3 certificates” on page 13.
- Support for preregistration, a process that enables one user, typically an administrator, to request a PKIX-compliant certificate for another user. Using the Trust Authority Client application, the end user can easily obtain the approved certificate without having to be knowledgeable about the enrollment process.
- Support for policy exits, which enables organizations to call their own programs during the enrollment process. The RA includes a sample policy exit that performs automated approval processing.

For complete information about using a Web browser or the Client application to enroll for certificates, see the Trust Authority User’s Guide. That book also describes the types of certificates provided in the default installation of Trust Authority.

**Administration**

The Registration Authority Desktop (RA Desktop) applet allows authorized administrators (registrars) to review applications for certificates, approve or reject requests, renew certificates, and permanently or temporarily revoke certificates. It supports such tasks as:

- Retrieving pending enrollment requests
- Querying the registration database to retrieve and act on records that match certain criteria
- Reviewing detailed information about a certificate or a request, such as the history of all actions taken since a request was first submitted
- Setting the validity period of a certificate
- Annotating a record to explain the reason for an action

The RA Desktop is a secure applet. To access it, a user must first become an authorized registrar. Trust Authority provides a tool to facilitate this process. You can add any number of users as registrars to support your registration work load.

When you add a registrar, you identify the registration domain and specify the user’s privileges. For example, you may allow one registrar to approve and reject requests only, but allow another registrar to revoke certificates as well.

- For information about installing, accessing, and using the RA Desktop applet, see the *Trust Authority RA Desktop Guide*.
- For information about authorizing registrars, see the *Trust Authority System Administration Guide*.

### Customization

You can use the registration facility provided with Trust Authority without customizing it. However, you probably want to change some of the enrollment forms or registration processes to reflect your organization’s specific goals for digital certification. For example, you may want to display your corporate logo on the browser enrollment form. You may also want to change certificate profiles to support extensions that are relevant to the class of users, servers, or devices you plan to enroll.

After you install and configure Trust Authority, you can copy many of the files that define your registration domain and customize them for your business purposes. As with any customization task, be sure to make a backup copy before changing a file.

You can copy or update the following registration facility files. During configuration, these files are created in the directory path established for your registration domain.

- The configuration files (file type .cfg) installed in the etc subdirectory. For example, you may want to adjust a runtime setting for the RA server or RA Desktop.
- The sample notification letters (file type .ltr) installed in the etc subdirectory. Trust Authority provides sample text to inform users when a request has been approved or rejected but you may want to write your own.
- The HTML files (file type .html), graphics (file type .gif), and Java® Server Pages (file type .jsp) installed in the webpages subdirectory. For example, you may want to alter the text and graphics displayed in the browser enrollment forms. You can also customize an existing certificate profile or define a new one to support your organization’s certificate policies.
- The policy exit (policy_exit) installed in the bin subdirectory. Trust Authority provides this exit as an example of how to handle automated approval processing. You can write other exits to integrate registration processing with your other applications or to process your own registration actions.
For information about changes you can make to your registration and certification processes, and for instructions on how to do so, see the Trust Authority Customization Guide.

Certificate Authority

The Certificate Authority (CA) is the server component that manages the certification process. The CA acts as a trusted third party to provide that users who engage in e-business can trust each other. It vouches for the identity of users through the certificates it issues. In addition to proving the identity of the user, the certificate includes a public key that enables the user to verify and encrypt communications.

In such a security model, the trustworthiness of the parties depends on the trust that is placed in the CA that issued the certificate. To ensure the integrity of a certificate, the CA digitally signs the certificate as part of creating it. Attempts to alter a certificate will invalidate the signature and render it unusable.

The Trust Authority CA provides a secure transaction environment in the following ways:

- To ensure the uniqueness of a certificate, the CA generates a serial number for each new certificate and for each renewed certificate. This serial number is a unique identifier that is not stored as part of the distinguished name (DN) in the certificate.
- To track the certificates it issues, the CA maintains an issued certificate list (ICL). The ICL stores a secure copy of each certificate, indexed by serial number, in a DB2 database.
- To track revoked certificates, the CA creates and updates certificate revocation lists (CRLs). The CA and RA exchange messages as soon as the revocation occurs, which enables the RA to update the Directory during the next periodic update. Just as it signs certificates, the CA digitally signs all CRLs to vouch for their integrity.
- To protect against data tampering, the CA computes a message authentication code (MAC) for each record written to the database. The MAC helps ensure the integrity of the database by enabling you to detect when data in it has been altered or deleted.
- To further protect the CA’s signature, the CA can be integrated with the IBM SecureWay 4758 PCI Cryptographic Coprocessor. The 4758 uses a cryptographic key stored in hardware to encrypt and protect the CA’s signing key.
- To support auditing and data recovery, the CA generates audit records for numerous auditable events. These records are stored in a DB2 database by the Audit server.
- If your organization has discrete applications for which a single CA would suffice, Trust Authority supports self-signed CA certificates. In this scenario, the CA is responsible for all of the certification activity within its administrative domain.
- If your organization has interleaving or hierarchical chains of authority, you can configure the CA to work with other CAs.
  - A Trust Authority CA can cross-certify with another CA and, in essence, agree to accept certificates signed by that CA as proof of authenticity. Cross-certification allows entities in one CA’s administrative domain to communicate securely with entities in another CA’s administrative domain.
  - A Trust Authority CA can serve as a root CA to sign other CA certificates. It also supports requests from other CAs that want to sign its CA certificate. This enables the CA to participate in a trust hierarchy; the CA agrees to accept certificates that are signed by any CA above it in the hierarchy as proof of authenticity.
Such trust models are useful, for example, for separating geographical areas and organizational units into distinct administrative domains. It also facilitates your ability to apply different certificate policies to different sections of the organization.

- If your organization needs certificates for purposes not already supported through the Trust Authority certificate profiles, the CA can generate and validate certificates with customer-defined extensions.

See the Trust Authority Customization Guide for information about defining new certificate profiles and certificate extensions.

For more detailed information about the Trust Authority CA, see the Trust Authority System Administration Guide. For example, that book contains guidelines for adjusting runtime options for the CA server and procedures for establishing cross-certified and hierarchical CA trust models.

**Audit subsystem**

In Trust Authority, the Audit subsystem provides support for logging security-relevant actions. The Audit server handles the following audit-related activity:

- It receives audit events from audit clients, such as the Registration Authority and Certificate Authority.

- It writes the events to an audit log that is typically stored in a DB2 database (you can choose to store the log as a data file). There is one record in the log per audit event.

- It allows the audit clients to mask certain audit events. Although some events are always logged, you can employ masking to prevent other events from being reported. This allows you to control the size of the audit logs and ensure that the logged events are ones that are of interest in your environment.

- It computes a message authentication code (MAC) for each audit record. The MAC helps ensure the integrity of the database contents. For example, you can determine whether a record has been altered, tampered with, or deleted since it was logged.

- It provides a tool for performing integrity checks on the audit database and archived audit records.

- It provides a tool for archiving and signing the current state of the audit database. For security purposes, you should archive the audit database and store it off-site on a periodic basis. Archiving the database can also provide performance benefits and conserve disk space.

The Audit server must be installed on the same machine with the Certificate Authority. After installing and configuring the system, see the Trust Authority System Administration Guide for information about using the audit tools and administering the Audit server.

**Web server**

Trust Authority uses the IBM WebSphere Application Server to provide a trusted base for network transactions. WebSphere is a security-aware collection of products, including the IBM HTTP Server, that supports the deployment of advanced e-business applications.

In a Trust Authority system, you must install the Web server software on the same machine as the Registration Authority. It provides a secure boundary between protected programs and the users who attempt to access them. Using Hypertext Transfer Protocols (HTTP and HTTPS) and Secure Sockets Layer (SSL) technology, the Web server can encrypt
communications between the clients and the server. It can also authenticate connections to prevent unauthorized access or data tampering.

The Web server uses different ports to handle different types of requests:

- A public port for requests that do not require encryption or authentication
- A secure port for requests that require encryption and server authentication
- A secure port for requests that require encryption, server authentication, and client authentication

In a Trust Authority system, the Web server handles all requests that it receives from a Web browser. This includes requests for new certificates, requests to renew or revoke existing certificates, and requests to run secure applets. If needed, it performs authentication before allowing any exchange of information to take place.

**Database system**

Trust Authority uses IBM DB2 Universal Database™ (DB2) as its storage base. The server components maintain separate databases for configuration data, registration data, certificate data, audit data, and Directory data. DB2 offers extensive security features and storage capacity. For example, it enables Trust Authority to store registration data in an encrypted format and to perform integrity checks on stored audit records.

The version of DB2 required by Trust Authority is included in the Trust Authority media package. Before installing the Trust Authority server code, you must ensure that the database software is available on each machine where you plan to install a server component. During installation and configuration, Trust Authority creates the needed databases for you.

**Directory server**

Trust Authority uses the IBM SecureWay Directory to maintain information about certificates in a centralized location. Through its integration with IBM DB2, the Directory can support millions of directory entries. It also allows client applications, such as Trust Authority, to perform database storage, update, and retrieval transactions.

In Trust Authority, the RA server publishes the following information in the Directory:

- Public key certificates, which are used for encryption and authentication
- The attributes associated with a distinguished name (the owner’s roles and privileges)
- Certificate revocation lists that include the serial numbers of all revoked certificates
- Information about the CA that signs the certificates, including the business and certificate policies associated with the certificate

**4758 cryptographic coprocessor**

When a CA issues a certificate, the CA’s signature certifies that the user is authorized to access the services for which the user registered. To prevent unauthorized users from obtaining certificates and gaining access to sensitive resources, you must protect the CA’s signing key.

By using encryption, software solutions can provide a high degree of security to the signing key. However, because the key must be in the clear to generate the signature, this approach exposes the key to capture by unauthorized users.
The IBM SecureWay 4758 PCI Cryptographic Coprocessor is special hardware that can be used in a Trust Authority system to protect CA keys. The 4758 coprocessor performs extensive RSA- and DES-based cryptographic functions within an enclosed, tamper-detecting, high-security processor on-board the hardware. It provides cryptographic data protection, key management, and custom application support. It also supports the MD5 and SHA-1 hash algorithms.

**Note:** Support for the 4758 coprocessor is provided only in the AIX® version of Trust Authority.

---

**Recommendation**

Although the 4758 coprocessor is not required, IBM recommends that you install it on the same server where you plan to install the Certificate Authority. If you rely on software to protect the CA keys, you cannot later install the hardware support without also reinstalling the Trust Authority software.

---

**Client application**

The Trust Authority Client application runs on the Microsoft Windows platform. This application provides the user interface for requests that use the PKIX Certificate Management Protocol (CMP). When a user submits a request to obtain, renew, revoke, or delete a certificate, the Client application communicates the request to the Registration Authority. When the RA issues a certificate, the application stores it on the user’s virtual or physical smart card.

In a typical Client scenario, an administrator gathers information about the user and, using the browser enrollment forms provided with Trust Authority, submits a preregistration request. When the request is approved, the RA returns either a transaction ID and a password, or a preregistration file and a password. The administrator then provides this information to the user.

While running the Client application, the user submits a request for the certificate and specifies the previously provided registration information. At that time, the application automatically installs the certificate on the user’s active smart card. With preregistration, the approval process takes place up front, at the time information about the user is collected, not at the time the certificate is issued.

Users can view summary information about all their certificates, including:
- The certificate’s status, such as whether it has been created or revoked
- The purpose of the certificate, such as whether it can be used for encryption
- The date the certificate is due to expire

Users can also view detailed information about individual certificates, including:
- The certificate’s encryption algorithm and key size
- The certificate’s validity period
- Information about the CA that issued the certificate

The Client application also allows users to use a certificate to digitally sign files, and to export certificates to existing PKI-aware applications such as Microsoft Internet Explorer or Netscape Communicator. This latter feature provides flexible and extensible support for multiple Internet-accessible applications, such as secure e-mail.
For information about installing, accessing, and using the Trust Authority Client application, see the Trust Authority User’s Guide.

**Key backup and recovery facility**

Trust AuthorityI provides a key backup/recovery request facility that enables backup and recovery of end entity certificates and corresponding private keys certified by Trust Authority.

By taking advantage of this facility, recovery of a lost, forgotten, or otherwise unobtainable certificate and private key is possible. Consider the following scenario for example: An employee routinely backs up their certificates and private keys and then suddenly leaves their company and fails to return all private keys required to access that information. By issuing a recovery quest, you can retrieve information once thought to be lost.

In general, the backup process entails the user creating a PKCS #12 file. This file contains the user’s certificate and private key. The user issues a backup request from a supported browser using the PKCS #12 file as input. The key recovery database, krbdb, gets updated and contains the access information. Key recovery works in a similar manner, in that you issue a recovery request specifying the password for the PKCS #12 file you backed up. Once the request is approved by the RA Administrator, the file is available for you to download.

**Architecture**

The following sections discuss the Trust Authority architectural framework and the protocols that it supports.

**Public key infrastructure**

The public key infrastructure (PKI) provides applications with a framework for performing the following types of security-related activities:

- Authenticate all parties that engage in electronic transactions
- Authorize access to sensitive systems and repositories
- Verify the author of each message through its digital signature
- Encrypt the content of all communications

The PKIX standard evolved from PKI to support the interoperability of applications that engage in e-business. Its primary advantage is that it enables organizations to conduct secure electronic transactions without regard for operating platform or application software package.

The PKIX implementation in Trust Authority is based on the Common Data Security Architecture (CDSA) from Intel Corporation. CDSA supports multiple trust models, certificate formats, cryptographic algorithms, and certificate repositories. Its primary advantage is that it enables organizations to write PKI-compliant applications that support their business policies.

**PKIX CMP protocol**

Trust Authority uses the PKIX Certificate Management Protocol (CMP) for communications between the RA and CA servers and for communications between the RA server and Trust Authority Clients. While CMP uses TCP/IP as its primary transport mechanism, an abstraction layer over sockets exists. This enables support for additional polling transports.

CMP defines message formats to support the entire certificate life cycle. It also specifies how message protection should be handled independent of the transport mechanism.
LDAP protocol

To provide applications with access to its centralized server services, the IBM SecureWay Directory supports the Lightweight Directory Access Protocol (LDAP). LDAP is a protocol that is derived from the X.500 standard. It runs over TCP/IP, and controls access through the use of distinguished names and passwords. Because it supports SSL connections, LDAP can also encrypt messages and perform mutual authentication of clients and servers.

In Trust Authority, the RA server uses LDAP to communicate with the Directory server. The RA publishes certificates, certificate revocation lists, and other information about registered entities and certification policies in the Directory on a scheduled periodic basis.

Object stores

Each Trust Authority component has an object store. The object store is a disk-based repository for persistent objects. It stores transactions in progress and state information about those transactions. The objects can be active control objects (such as certificates, requests, and CRLs), or surrogates. A surrogate is an area where state data about the object is saved.

For example, when a Client user requests a certificate, the CertRequest control object moves from the Client system to the RA server. However, the Client must store some state data (for example, an encryption key) so that it can decode the fulfilled CertRequest when it returns. To achieve this, the Client maintains a surrogate of the request when it forwards the active CertRequest control object to the RA. When the fulfilled CertRequest object returns, the Client automatically deletes the surrogate.

Because objects in the object store are stored in an ASN.1-encoded format, retrieval and storage can be a relatively expensive operation. The object store caches modifications to objects, and does not update the disk storage until a change in object state occurs, or until a user interface alters the object.

To minimize the overhead that is associated with ASN.1 parsing, Trust Authority uses an object-cache layer above the object store that performs a write-through cache of object store objects. As a result, an object requires parsing only the first time it is referred to after a server restart.

The object cache layer provides an additional per-object storage area which is not disk based. Trust Authority uses this area for storing transient, security-related information, such as the password under which a preregistration record is protected. The object cache can also lock record objects to protect against simultaneous access by multiple threads.

Smart card support

Smart cards are portable cryptographic devices, typically the size of a credit card, that store certificates and keys. They can perform cryptographic operations without releasing the private key from the card.

Trust Authority uses PKCS #11 version 2.01 to support virtual smart card operations. PKCS #11 provides functionality for key pair generation, data storage, and signing.

Users can obtain certificates for smart cards by enrolling through Netscape Navigator or Netscape Communicator, version 4.6 or later. Because not all users have access to smart card hardware, the Trust Authority Client includes a virtual smart card that acts the same as a physical smart card.
Trust model

Security in a Trust Authority system is done through the use of code signing, message signing, data encryption, and the secure storage of keys and passwords.

Code signing

Core Trust Authority code is signed at the time it is manufactured. When code is signed with a factory-generated private key, it becomes a static and protected object. It cannot be altered or replaced without detection. Other code objects are able to use the corresponding public key and the internal verification library to authenticate the communication before any exchange of data takes place.

Message signing

To provide even greater authentication services, the configuration process generates signing keys for the RA, CA, and Audit servers. This provides that all inter-component communications are signed. For example, all messages exchanged between the RA and CA can be authenticated on the basis of each component’s signature.

Data encryption

All information stored in KeyStores is encrypted. By using DB2, much of the information stored in the Trust Authority databases is also encrypted.

KeyStores

Trust Authority provides support for KeyStores, secure areas that store private keys, certificates, message authentication codes (MACs), and other security-relevant objects. Distinct KeyStores exist for the CA and Audit components and for several server agents that help carry out server transactions. Information in each KeyStore is encrypted and accessible only through a password that is established for that KeyStore.

This trust model helps ensure system integrity by protecting objects that are stored in KeyStores. It also helps ensure the confidentiality of those objects by allowing only a trusted system component — one that was signed with a factory-generated key — to access the KeyStore and the encrypted data in it.

During configuration, there are two passwords you set. They are the cfguser password and the control program password. These passwords can be the same or different. After configuration, you must set a unique password for each KeyStore. See the Trust Authority System Administration Guide for information about using the Change Password utility to make these changes.

Supported standards

IBM SecureWay Trust Authority supports the following standards for public key cryptography.
<table>
<thead>
<tr>
<th>Component</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration Authority</strong></td>
<td>■ Secure Sockets Layer (SSL) version 2 and version 3, with client authentication</td>
</tr>
<tr>
<td></td>
<td>■ PKCS #10 browser and server certificate format, with a Base64-encoded PKCS #7 response</td>
</tr>
<tr>
<td></td>
<td>■ PKIX CMP certificate format, with a PKIX CMP response</td>
</tr>
<tr>
<td></td>
<td>■ IPSec certificate format</td>
</tr>
<tr>
<td></td>
<td>■ S/MIME certificate format</td>
</tr>
<tr>
<td></td>
<td>■ Browser certificates for:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer versions 4.x and 5.x</td>
</tr>
<tr>
<td></td>
<td>■ Netscape Navigator and Netscape Communicator versions 4.x</td>
</tr>
<tr>
<td></td>
<td>■ Server certificates for:</td>
</tr>
<tr>
<td></td>
<td>■ Netscape Enterprise Server</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Information Server</td>
</tr>
<tr>
<td></td>
<td>■ Smart card certificates (PKCS #11 interface) for:</td>
</tr>
<tr>
<td></td>
<td>■ Trust Authority Client application</td>
</tr>
<tr>
<td></td>
<td>■ Netscape Navigator and Netscape Communicator versions 4.x</td>
</tr>
<tr>
<td></td>
<td>■ LDAP standard for communications with the Directory</td>
</tr>
<tr>
<td></td>
<td>■ PKIX CMP via TCP/IP for communications with the Certificate Authority</td>
</tr>
<tr>
<td></td>
<td>■ PKIX CMP via TCP/IP for communications with the Client application</td>
</tr>
<tr>
<td><strong>Certificate Authority</strong></td>
<td>■ X.509v3 certificates</td>
</tr>
<tr>
<td></td>
<td>■ Certificate revocation lists (CRLv2)</td>
</tr>
<tr>
<td></td>
<td>■ Key lengths up to 1024 bits for encryption and key exchange keys</td>
</tr>
<tr>
<td></td>
<td>■ Key lengths up to 2048 bits for CA signing keys</td>
</tr>
<tr>
<td></td>
<td>■ RSA algorithms for encryption and signing</td>
</tr>
<tr>
<td></td>
<td>■ MD5 and SHA-1 hash algorithms</td>
</tr>
<tr>
<td></td>
<td>■ PKIX CMP via TCP/IP for communications with theRegistration Authority</td>
</tr>
<tr>
<td><strong>SecureWay Directory</strong></td>
<td>LDAP version 3.1.1.5, with RFC 1779 syntax</td>
</tr>
<tr>
<td><strong>IBM SecureWay 4758 PCI</strong></td>
<td>■ FIPS 140 level 4 requirements for resistance to physical attacks</td>
</tr>
<tr>
<td><strong>Cryptographic Coprocessor Hardware</strong></td>
<td>■ Support for industry-accepted cryptography standards:</td>
</tr>
<tr>
<td></td>
<td>■ DES for encryption/decryption</td>
</tr>
<tr>
<td></td>
<td>■ RSA for signing/signature verification</td>
</tr>
<tr>
<td></td>
<td>■ PKCS #1 block type 00</td>
</tr>
<tr>
<td></td>
<td>■ PKCS #1 block type 01</td>
</tr>
<tr>
<td></td>
<td>■ PKCS #1 block type 02</td>
</tr>
<tr>
<td></td>
<td>■ MD5 and SHA-1 hash algorithms</td>
</tr>
<tr>
<td></td>
<td>■ X9.9 and X9.23 ANSI</td>
</tr>
<tr>
<td></td>
<td>■ ISO 9796</td>
</tr>
<tr>
<td><strong>IBM CCA Cryptographic</strong></td>
<td>Provides services for the 4758 coprocessor, including the secure generation of RSA key pairs with modulus lengths as long as 2048 bits, and:</td>
</tr>
<tr>
<td><strong>Coprocessor Support Program</strong></td>
<td>■ SET (Secure Electronic Transaction)</td>
</tr>
<tr>
<td></td>
<td>■ DES for encryption and decryption</td>
</tr>
<tr>
<td></td>
<td>■ RSA for signing and signature verification</td>
</tr>
<tr>
<td></td>
<td>■ MD5 and SHA-1 hash algorithms</td>
</tr>
</tbody>
</table>

**X.509 version 3 certificates**

Trust Authority certificates support most of the fields and extensions defined in the X.509 version 3 (X.509v3) standard. This support enables the certificates to be used for most cryptographic purposes, such as SSL, IPSec, VPN, and S/MIME.

Trust Authority certificates can include the following types of extensions:
Standard Extensions
The standard X.509v3 certificate extensions: key usage, private key usage period, subject alternative name, basic constraints, and name constraints.

Common Extensions
Extensions that are unique to Trust Authority, such as host identity mapping. This extension associates the subject of a certificate with a corresponding identity on a host system.

Private Extensions
Extensions that an application can use to identify an online validation service that supports the issuing CA.

To support your organization’s registration policies, Trust Authority also provides the means for you to customize and define certificate extensions. For example, you can change the extensions that are specified in the default certificate profiles, or create profiles that return certificates with different extensions.

For complete information about creating or customizing certificate extensions and certificate profiles, see the Trust Authority Customization Guide.

Related information
The Trust Authority product documentation is available in Portable Document Format (PDF) and HTML format on the IBM SecureWay Trust Authority Documentation CD-ROM. HTML versions of some publications are installed with the product and are accessible from the user interfaces.

Be aware that the product may have changed since the publications were produced. For the latest product information, and for information about accessing a publication in the language and format of your choice, see the Readme file. The latest version of the Readme file is available at the IBM SecureWay Trust Authority Web site: http://www.tivoli.com/support

The Trust Authority library includes the following documentation:

Up and Running
This book provides an overview of the product. It lists the product requirements, includes installation procedures, and provides information about how to access the online help available for each product component. This book is printed and distributed with the product.

System Administration Guide
This book contains general information about administering the Trust Authority system. It includes procedures for starting and stopping the servers, changing passwords, administering the server components, performing audits, and running data integrity checks.

Configuration Guide
This book contains information about how to use the Setup Wizard to configure a Trust Authority system. You can access the HTML version of this guide while viewing online help for the Wizard.

Registration Authority Desktop Guide
This book contains information about how to use the RA Desktop to administer
certificates throughout the certificate life cycle. You can access the HTML version of this guide while viewing online help for the Desktop.

User’s Guide
This book contains information about how to obtain and manage certificates. It provides procedures for using the Trust Authority browser enrollment forms to request, renew, and revoke certificates. It also discusses how to preregister for PKIX-compliant certificates, and how to use the Trust Authority Client to manage these certificates. You can access the HTML version of this guide while viewing online help for the Client.

Customization Guide
This book shows you how to customize the Trust Authority registration facility to support the registration and certification goals of your business policies. For example, you can learn how to customize HTML and Java Server pages, notification letters, certificate profiles, and policy exits.

The Trust Authority Web site includes other documents that may help you install, administer, and use Trust Authority. For example, you can find supplemental guidelines on the Directory schema and learn how to integrate Trust Authority with the IBM SecureWay 4758 PCI Coprocessor.

Year 2000 readiness
IBM SecureWay Trust Authority is Year 2000 ready. When used in accordance with its associated documentation, it is capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided that all products (for example, hardware, software, and firmware) used with the product properly exchange accurate date data with it.

Service and support
The latest information about Trust Authority is always available in the Readme file. Before contacting IBM for support, make sure that you have the latest version of this file. To obtain the Readme file, access the IBM SecureWay Trust Authority Web site:
http://www.tivoli.com/support

The Trust Authority Web site contains other supplemental guidelines, such as information about how to integrate Trust Authority with other products in your environment.

If the Readme file does not answer your questions, contact the IBM Support Desk at the following telephone number:
1-800-237-5511

Note that you can request IBM Support only if you have a valid customer number and have a support entitlement in place.

Trust Authority occasionally publishes minor code fixes and Corrective Service Disks as needed. To obtain the latest software patch, access the Trust Authority Support page:
http://www.tivoli.com/support/downloads
At the Downloads page, there are a number of links. The links that require you to enter a userid and password are referred to as "restricted". You can obtain a userid and password for that Web site upon completing a registration form located at the following Web site:
http://www.tivoli.com/support/custreg/custreg.html
System requirements

Your operating environment must meet the software and hardware requirements that are discussed in the following sections. For the latest information about system requirements, see the Trust Authority Readme file. That file may contain information that supersedes the product publications.

To obtain the most current Readme file, access the IBM SecureWay Trust Authority Web site.

Server software requirements

To distribute the work load among processors, and to support your organization’s existing system configuration, you can install the Trust Authority server programs on multiple machines. For a discussion of different ways you might want to set up Trust Authority in your environment, see “Supported server configurations” on page 28.

The following table summarizes the Trust Authority operating system and software requirements.

<table>
<thead>
<tr>
<th>Product</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>One of the following operating systems:</td>
<td>Required.</td>
</tr>
<tr>
<td>■ IBM AIX/6000® (AIX), version 4.3.3</td>
<td>■ You must install all Trust Authority server programs on the same platform. You cannot mix AIX and Windows NT machines in a single Trust Authority installation.</td>
</tr>
<tr>
<td>■ Microsoft Windows NT, version 4.0 with Service Pack 5.</td>
<td></td>
</tr>
<tr>
<td>IBM DB2 Universal Database</td>
<td>Required; provided in the Trust Authority media package.</td>
</tr>
<tr>
<td>■ A unique database exists for each Trust Authority server component.</td>
<td>■ Before installing Trust Authority, you must install DB2 on each machine that you plan to use as a Trust Authority server.</td>
</tr>
<tr>
<td>IBM WebSphere Application Server, Standard Edition. Includes the IBM HTTP Server and Sun Java Development Kit (JDK)</td>
<td>■ Required; provided in the Trust Authority media package.</td>
</tr>
<tr>
<td>■ Before installing Trust Authority, you must install the Web server software on the same machine where you plan to install the Registration Authority.</td>
<td></td>
</tr>
</tbody>
</table>
Product Notes
IBM SecureWay Directory
- Required; provided in the Trust Authority media package.
- Before installing Trust Authority, you must install the Directory software. You can install it on the same machine with Trust Authority, or you can install it on a remote machine.

- IBM SecureWay 4758 PCI Cryptographic Coprocessor
- IBM SecureWay 4758 CCA Support Program
- Optional, and available only for AIX systems; you must order this product through normal IBM ordering channels.
- Before installing Trust Authority, you must install the 4758 hardware and support program on the server where you plan to install the Certificate Authority.
- The 4758 cryptographic card requires a PCI bus on the RS/6000®.

**Server hardware requirements**

The machine configuration you choose for Trust Authority depends on your anticipated business activity and whether you intend to use Trust Authority in AIX or Windows NT.

- If you plan to run Trust Authority under AIX, you must install it on an IBM RISC System/6000® (RS/6000®) machine.
- If you plan to run Trust Authority under Windows NT, IBM recommends that you install it on an IBM Netfinity® Server.

Use the following definitions as a guideline when assessing your capacity and throughput requirements:

- **Small Production or Test Environment**
  A site that issues hundreds of certificates per day. This may be a system set up to issue certificates to employees through an intranet, or a system set up for test and application development purposes.

- **Medium Production Environment**
  A site that issues thousands of certificates per day. This may be a system that is set up by small and medium businesses to issue certificates over the Internet.

- **Large Production Environment**
  A site that issues many thousands of certificates per day. This may be a system that is set up by a large business to issue certificates over the Internet. It may also be a system that provides third-party CA services to other organizations.

The following table summarizes the recommended machine requirements for a small production environment. You should adapt your physical machine configuration in accordance with your anticipated processing needs.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Machine Type</th>
<th>Processors</th>
<th>Disk Space</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>RS/6000</td>
<td>1 (233 MHz)</td>
<td>2 GB</td>
<td>256 MB</td>
</tr>
</tbody>
</table>
Setup Wizard requirements

IBM recommends the following workstation configuration for running the Trust Authority configuration applet (called the Setup Wizard).

- The following physical machine setup:
  - Intel Pentium processor with at least 64 MB of RAM, or better
  - A computer display that supports 1024x768 or higher resolutions at 65536 colors, or better

- One of the following operating systems:
  - IBM AIX
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT

- A Web browser that supports JDK 1.2.2–based applets, such as the following. You must install the official version of the browser as distributed by Netscape or Microsoft. Versions obtained from third-party vendors may not display information correctly, especially when running an applet in a language other than English.
  - Netscape Navigator or Netscape Communicator, version 4.05 or later for Windows platforms and version 4.5 for AIX.
  - Microsoft Internet Explorer, version 5.0

- The Java Swing Library (swingall.jar), version 1.2.2, locally installed. When you first start the Setup Wizard, you see instructions for how to download and install the required version of this library.

The following table summarizes the general software requirements and the versions required:

Table 1. General software requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Netscape</th>
<th>Internet Explorer</th>
<th>JDK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT</td>
<td>4.05</td>
<td>5.0</td>
<td>1.1.6.0 or greater</td>
</tr>
<tr>
<td>Windows 95</td>
<td>4.05</td>
<td>5.0</td>
<td>1.1.6.0 or greater</td>
</tr>
<tr>
<td>Windows 98</td>
<td>4.05</td>
<td>5.0</td>
<td>1.1.6.0 or greater</td>
</tr>
<tr>
<td>AIX</td>
<td>4.5.1</td>
<td>N/A</td>
<td>1.1.6.7</td>
</tr>
</tbody>
</table>

Note: For AIX, install the IBM Developer Kit for AIX, Java Technology Edition, version 1.2.2 (also referred to as JDK) from the WebSphere CD-ROM that accompanies the Trust Authority product.
The following table summarizes specific software requirements and the versions required:

**Table 2. Specific software requirements**

<table>
<thead>
<tr>
<th>Browser</th>
<th>RA Desktop</th>
<th>Setup Wizard</th>
<th>DC attribute (used in DNs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netscape</td>
<td>4.51</td>
<td>4.05</td>
<td>4.7</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
</tr>
</tbody>
</table>

See the *Trust Authority Configuration Guide* for complete information about running the Setup Wizard and configuring your Trust Authority system.

**Client requirements**

To determine whether your workstation meets the requirements for running the Trust Authority Client application or using a browser to request and manage certificates, see the *Trust Authority User’s Guide*.

To determine whether your workstation meets the requirements for running the Trust Authority RA Desktop, see the *Trust Authority RA Desktop Guide*. 
Planning for Trust Authority

This chapter discusses how IBM SecureWay Trust Authority interacts with its prerequisite products. You should review this information before you install and configure Trust Authority. It also includes guidelines for preparing the operating environment for how you intend to use Trust Authority. It includes the following topics:

- How to **secure the system** to protect it physically and to protect it from unauthorized electronic intrusion
- How to **configure IP aliases** for the Web server to support your organization’s firewall requirements
- How Trust Authority **creates and uses databases**
- How Trust Authority **interacts with the Directory**
- How Trust Authority **interacts with the 4758 coprocessor**
- How Trust Authority **interacts with Policy Director**
- **Suggested server configurations** for running Trust Authority in a multiple machine environment
- **National language considerations** for running Trust Authority in your organization’s language locale
- **A summary of the CD-ROMs provided in the Trust Authority product distribution package**

**Securing the system**

Trust Authority uses encryption, digital signatures, and digital certificates to protect transactions and to protect your resources from unauthorized intrusion. However, the security of the Trust Authority server itself is dependent on the security of its underlying operational environment.

This section provides suggestions for securing the physical environment of your system to minimize penetration by unauthorized users before you begin to install the Trust Authority software. A discussion of using firewall technology follows.

**Isolated Area**

Set up the server in an isolated room that is dedicated to CA activity. If possible, the room should have reinforced walls, a single solid-core wood or steel door, and a solidly constructed ceiling with no drop panels. The room should also have a raised floor to protect against discharges in the event of a fire.
**Maintained Area**

The room should provide an uninterruptible power supply (UPS) for the computers, light fixtures, motion detectors, and heating and cooling systems. Monitor the room’s temperature controls to ensure that cool air flow is sufficient to offset the heat that is generated by the equipment.

**Controlled Access**

You can provide access to the physical area in a number of ways, for example, by using badges or keypad-controlled door locks. To prevent malicious tampering by a single individual, you should install controls that require the presentation of proper credentials by at least two trusted employees.

You should also monitor the room to track each time the secure area is accessed and by whom. For maximum security, install motion detectors both inside and outside the door.

**Controlled Communications**

There should be no spare open ports on the Trust Authority server. You should configure the system so that it listens for requests only on those ports that are explicitly assigned to active Trust Authority applications.

**Using firewall technology**

IBM strongly recommends that you install a firewall, such as IBM SecureWay Firewall, to protect the Trust Authority system from intrusion through another part of your network. A firewall allows you to secure the system in the following ways:

- Control which applications are able to access your internal network from the Internet
- Control which addresses on your internal network an authorized application can access
- Prevent internal applications from accessing the external (Internet) network
- Authenticate the sources of all incoming requests and permit or deny access accordingly

To enforce access restrictions, you should configure the Trust Authority servers behind the firewall. You should ensure that the firewall you install provides the following functionality, at a minimum:

- A screening router to selectively block data packets according to your policy preferences. For example, your firewall should allow you to establish controls that restrict communications to specific IP addresses and ports.
- A proxy server to act as an intermediary between client/server requests. For example, your firewall should allow you to intercept FTP or HTTP requests from users before routing them to the appropriate server process. Doing so prevents the client and server from communicating directly with each other.
- A perimeter network to provide an extra buffer that can segregate and protect the internal network in the event that the external network is compromised.

Keep in mind that you can install the Trust Authority server programs on multiple machines — an arrangement that provides several advantages. For example, you can achieve performance improvements by spreading the work load across multiple processors, set up separate backup schedules, and control access to different processes through IP address mapping. To ensure the security of these programs, however, you must configure these servers behind the firewall. You should take the same precautions to protect them that you do to protect the main server.
Working with Trust Authority databases

Trust Authority uses IBM DB2 Universal Database software to manage data. The version of DB2 included in the Trust Authority media package is intended solely for use by Trust Authority applications. If you want to customize the database software, or use it for purposes other than Trust Authority, you must purchase a license for a complete version of IBM DB2 Enterprise Edition.

If you plan to set up Trust Authority in a multiple machine configuration, you must install the Trust Authority database software on each machine where you plan to install a Trust Authority server component.

As part of running a post-installation configuration program, Trust Authority creates the following database for configuration data, and populates the database with default configuration values:

- `cfgdb`

During configuration, Trust Authority creates the following databases for CA data, registration data, and audit data. If you install Trust Authority on AIX, you must create disk partitions for these databases before you start the installation process. See “Set up AIX disk partitions” on page 33 for details.

- `ibmdb`
- `pkrfdb`
- `adtdb`
- `krdbname`

Unless it already exists, Trust Authority also creates the following database for the Directory:

- `ldapdb`

If you install all the server components on the same machine, the configuration programs will create the databases in the background. If you install the CA, Audit, or Directory components on remote machines, there are steps you must take during configuration to ensure that the databases are properly instantiated. The Trust Authority Configuration Guide discusses these remote configuration procedures.

If you install Trust Authority on AIX, the configuration, CA, registration, and audit databases are created under an instance named `cfguser`. Unless a database for the Directory was previously created, it is created under an instance named `ldapInst`.

If you install Trust Authority on Windows NT, the instance name for the Trust Authority databases matches the username under which you install the product (the suggested value is `cfguser`, but your installation may be different). Unless a database for the Directory was previously created, it is created under an instance named `ldapInst`.

To support backup and recovery, Trust Authority enables audit logging for registration and certification events. See the Trust Authority System Administration Guide for guidelines on how to archive the audit logs and how to back up and restore the system. For additional information about how to back up and restore the databases, consult with your local DB2 database administrator.
Configuring IP aliases for the Web server

The IBM SecureWay Trust Authority media package includes the Web server software you need for Trust Authority: IBM WebSphere Application Server, IBM HTTP Server, and the Sun Java Development Kit (JDK). After installing this software, you may want to configure particular ports for processing public and secure requests.

In a Trust Authority system, the Web server needs to support three kinds of requests:

- Non-SSL, or public requests.
- Secure SSL requests without client authentication.
- Secure SSL requests with client authentication.

In the default configuration, Trust Authority designates ports on the Web server to handle each type of request. This enables you to use the system as installed without making special adjustments to your network configuration.

The following table summarizes this architecture and the default port values.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>SSL</th>
<th>Server Authentication</th>
<th>Client Authentication</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>443</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>1443</td>
</tr>
</tbody>
</table>

In many secure systems, only ports 80 and 443 can be open through the firewall and only port 443 can be used for an SSL connection. If this is the case for your organization, you need to configure the Web server so that different types of requests can be processed through the same port. For example, you may want to configure the system so that both secure servers listen for requests at port 443.

To provide multiple access points to the same machine through the same port, you need to define virtual host names and associate them with IP addresses that are aliases of the machine’s real IP address. This concept, known as IP aliasing, allows you to run multiple independent servers on a single machine.

**Note:** If you do not intend to use the default configuration values for the Web server ports, you must configure the IP aliases before you run the Trust Authority configuration applet. The configuration programs rely on these values when creating the CA certificate for your system.

You set up IP aliases in your TCP/IP Domain Name Services (DNS). For Trust Authority, you might want to configure two aliases:

- Configure DNS and specify the machine’s host name and IP address. Use this entry for the public server that listens for non-SSL requests at port 80.
- Add an alias (virtual) host name and an alias IP address. Use this entry for the secure Web server that listens for SSL, non-client-authenticated requests at port 443.
- Add a second alias host name and a second alias IP address. Use this entry for the secure Web server that listens for SSL, client-authenticated requests at port 443.
Note that these alias host names and IP addresses must be unique and they must map to the same physical machine.

For information about configuring virtual host names and IP aliases, consult the documentation provided with your DNS product. You can also review documentation available for the IBM HTTP Server. For example, access the User Assistance information available at the following IBM HTTP Server URL:

Working with the Directory

The IBM SecureWay Trust Authority media package includes the software you need for the Directory. You can install the software provided with Trust Authority and set it up specifically for use with Trust Authority, or you can use Trust Authority with an existing Directory. When you install the Trust Authority server software, the installation programs update the Directory with information that is required by the Trust Authority components.

During configuration, Trust Authority creates entries that it needs to be able to bind to the Directory and publish information. For example, the configuration program creates an entry for the Trust Authority CA and assigns the appropriate Directory access permissions.

If you install all the server components on the same machine, the configuration programs will install or update the Directory in the background. If you install the Directory on a remote machine, there are steps you must take during configuration to ensure that it is properly configured. The Trust Authority Configuration Guide discusses this procedure.

Note: Before installing or configuring the Directory, consult "Using the SecureWay Directory With Trust Authority". This document, which provides guidelines for setting up the Directory for a Trust Authority system, is available at the IBM SecureWay Trust Authority Web site.

Directory schema

Each entry in the Directory represents a single object, such as a person, organization, or device, that is identified by a unique and unambiguous distinguished name (DN). The Directory schema defines the rules for DNs, such as how to declare them and the types of information that may or must be included.

The DN contains a set of attributes that help to uniquely identify the object and delineate the object’s privileges. Attributes, for example, may identify where the object is located, the organization that the object is affiliated with, and the name the object is known by.

To help you define the Directory entries that Trust Authority needs, the configuration applet provides a graphical user interface. The Distinguished Name Editor allows you to specify DN attributes without having to be aware of Directory schema requirements.

Directory access controls

All Directory entries are logically organized into a hierarchical structure that is called the Directory Information Tree (DIT). This tree has a single root and an unlimited number of cascading nodes. Each node corresponds to a Directory entry that is identified by a distinguishing attribute.
The Directory allows access control privileges to be set for an individual entry or for an entry and its entire subtree. When you configure Trust Authority, it automatically applies the appropriate privileges for each Trust Authority DN entry. To summarize:

- The Certificate Authority needs to be able to access all entries at or below its DN entry point in the Directory hierarchy. Objects at or below the CA’s base level are members of the CA’s administrative domain. They represent the entities that are authorized to receive a public key and certificate certified by the CA.

- Because the Trust Authority CA does not directly bind to the Directory, it uses an agent called the Directory administrator. The Directory administrator carries out requests between the CA, RA, and Directory. It is authorized to update all entries in the CA’s subtree in the Directory. This privilege includes the ability to add, delete, change, read, search, and compare Directory entries.

- Each Trust Authority system also defines a Directory root DN. The root DN is a configured entity that does not actually exist in the Directory tree. As the root administrator, it has the authority to update all nodes in the Directory, not just those in a particular CA’s subtree.
  Attributes in the root DN describe the protocols and controls supported by the Directory. This allows clients such as Trust Authority to determine basic information about the server and the Directory tree. It also enables Trust Authority to bind to the Directory to make changes to it.

### Working with the 4758 coprocessor

Although this product is optional, you are encouraged to use the IBM SecureWay 4758 PCI Cryptographic Coprocessor to help maximize the security of CA signing keys. Doing so can help minimize your exposure to harm from abusive system administrators or system infiltrators.

**Note:** Support for the 4758 coprocessor is provided only in the AIX version of Trust Authority.

The 4758 coprocessor uses the IBM Common Cryptographic Architecture API to provide strong cryptographic services. All cryptographic processing occurs within the secure boundaries of the physical cryptographic card.

During installation, the 4758 configuration program generates a master key and stores it in hardware. In a Trust Authority system, the coprocessor uses this master key, and an RSA algorithm, to triple-encrypt the CA’s signing key. This step provides an extra layer of security against attempts to compromise or otherwise decipher the CA’s signature.

In addition to its cryptographic intelligence, the 4758 coprocessor can detect attempts to tamper with the hardware or master key, irregularities in voltage and temperature, and excess radiation. On detection, the keys required to access data that is secured in the module are destroyed.

**Note:** For information about installing, configuring, and cloning the 4758 coprocessor, see "*Using the SecureWay 4758 Coprocessor With Trust Authority*". This document is available at the [IBM SecureWay Trust Authority](https://www.ibm.com) Web site.
Storing the CA key in hardware

If you decide to use the 4758 coprocessor, you must install it on the machine where you installed the Trust Authority CA server before configuring the Trust Authority system. As part of configuring the CA, you specify whether or not it should use the coprocessor to store its signing key.

In most Trust Authority systems, the CA’s key is not physically stored with the master key. However, a configuration option allows you override this default — an action that IBM discourages. If the 4758 coprocessor hardware fails, you need to be prepared to take immediate corrective action.

If you choose to store the CA’s key in hardware, you should prepare a disaster recovery plan. You need to understand the risks and corrective actions associated with this decision:

- When the 4758 coprocessor is backed up, only its master key is backed up, not any other keys stored on the hardware card. Therefore, if the card is damaged or some other hardware failure occurs, you will lose the CA’s signing key.
- If the CA’s key is lost or compromised, you must take the CA down and bring it up with a new key. While the CA is unavailable, users whose certificates are signed by the CA cannot use them because there is no means to validate them.
- Because the certificates that were signed with the CA’s original key are no longer valid, you must issue new certificates signed with the new CA key after you re-establish the CA.

Integration with Policy Director

IBM SecureWay Policy Director provides end-to-end security for resources that span geographically dispersed intranets and extranets. It includes extensive support for authentication, authorization, data security, and resource management. By integrating Policy Director with Trust Authority, you can create a secure and certificate-protected environment for your e-business activities.

Policy Director provides a single point of control for Web environments. When a user attempts to access a secure site, Policy Director can require a single sign-on for each Web user, authenticate the user’s identity, and verify the user’s authority to access a protected area. As part of this validation process, Policy Director can be configured to evaluate Trust Authority certificates.

For example, you can configure Policy Director to accept only those certificates that have been signed by a trusted CA — one that is known to Policy Director. By providing Policy Director with a Trust Authority CA certificate, you can easily establish a trustworthy barrier between unauthorized users and the resources you need to protect.

For information about using Trust Authority certificates in a Policy Director environment, see IBM SecureWay FirstSecure Planning and Integration. That book also tells you how to provide Policy Director with the information it needs to authenticate certificates that are signed by the Trust Authority CA.
**Supported server configurations**

You can install all the Trust Authority server components on a single machine or distribute the processing among multiple machines. Certain components, however, must co-exist on the same machine:

- The main Trust Authority server, which includes the administrative programs, the Web server, the RA server, and the databases that hold configuration and registration data.
- The CA server and Audit server, and their respective databases.
- The Directory server and its database.

How you configure your server network depends on your organization’s anticipated workload and whether you use a particular machine for multiple purposes. For example, if you previously installed the Directory and use it with other applications, you might want to keep that server remote from the other Trust Authority components.

The following configurations summarize the ways that you can distribute the server components.

- The main Trust Authority server, the CA and Audit servers, and the Directory server on one machine.
- The main Trust Authority server, the CA and Audit servers, and the Directory server on three separate machines.
- The main Trust Authority server on one machine, with the CA and Audit servers and the Directory server on a second machine.
- The main Trust Authority server and CA and Audit servers on one machine, with the Directory server on a second machine.
- The main Trust Authority server and Directory server on one machine, with the CA and Audit servers on a second machine.

**International environment considerations**

The Trust Authority components have been enabled for deployment in an international environment. For example:

- Message files and graphical user interfaces are translated and provide national language support in ten languages: English, French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, and Traditional Chinese.
- All textual input fields support Unicode through UTF-8 encoding.
- All distinguished names support Unicode through UTF-8 encoding.

In Trust Authority, the following items are available in English only:

- Some of the product publications.
- All directory paths in the configuration files, which must be specified in ASCII format.

Because of government export regulations, the Trust Authority product is distributed in separate encryption editions. The edition available to domestic customers (U.S., U.S. Subsidiaries, and Canada) includes a stronger encryption algorithm than the edition that is
made available to international customers. The cryptographic algorithms are predetermined in the product code and cannot be altered when you install, configure, or use the product.

**Trust Authority media package**

Software for the Trust Authority product is distributed in a media package that contains the following CD-ROMs:

1. *IBM WebSphere Application Server for AIX Standard Edition V3.5 Application Server and IBM HTTP Server CD*
   This CD-ROM contains the Web server software that is required for Trust Authority. It includes the Application Server and the IBM HTTP Server.

   This CD-ROM contains the Directory software that is required for Trust Authority.

3. *IBM SecureWay Trust Authority for AIX, Disk 1*
   This CD-ROM contains the database software that is required for Trust Authority.
   Platform-specific CDs are provided for AIX.
   - The Trust Authority Registration Authority, Certificate Authority, and Audit server programs; Directory-related software; and programs for installing, configuring, and administering the product.
   - Fix pack software for the Trust Authority database programs.
   - WebSphere Application Server software.
   - An installation image for the Trust Authority Client application.
   - An installation image for the Trust Authority Registration Authority Desktop applet.

4. *IBM SecureWay Trust Authority Documentation CD*
   This CD-ROM contains HTML and PDF versions of all Trust Authority product documentation.

5. *IBM SecureWay Trust Authority Up and Running V3.7*
Installing Trust Authority on AIX

This chapter provides procedures for installing Trust Authority and its prerequisite products on an AIX platform.

Before you begin installing software for Trust Authority, be sure to read the latest version of the product Readme file. To obtain the most current version of this file, access the IBM SecureWay Trust Authority Web site:
http://www.tivoli.com/support

Note: The main procedures in this chapter assume that you are installing Trust Authority for the first time. Before installing Trust Authority it is highly recommended that you back up the data files before beginning. Refer to the instructions in “Run the backup utility” on page 46 for backing up your data files. Following the backup, proceed with the Trust Authority installation.

Tivoli recommends that you install software for Trust Authority in the following order:

1. AIX operating system version 4.3.3.
2. IBM DB2 Universal Database version 6.1 fp3
3. IBM SecureWay Directory Server version 3.1.1
4. IBM Developer Kit for AIX, Java Technology Edition, version 1.2.2.0, and the xIC runtime environment version 3.6.4.1.
5. IBM WebSphere Application Server Standard Edition version 3.5.0
6. Upgrade GSKIT to version 4.
7. Upgrade IBM HTTP Server (IHS) to version 1.3.3.1
8. Start the WebSphere Application Server
9. KeyWorks
10. Trust Authority server software, which includes the core server programs.

**Multiple Machine Configuration**

If you are not installing all the server software on the same machine, you must repeat the procedures below to install AIX and the Trust Authority database software on each component machine.
Setting up AIX

Use the following guidelines when installing AIX software on the machine or machines where you plan to install Trust Authority software. If you previously installed AIX, use these guidelines as a checklist to make sure that you installed all the files that are required by the Trust Authority components.

If you are setting up Trust Authority in a multiple machine configuration, you must install AIX on each machine where you plan to install a Trust Authority server component.

- Log in as root.
- Perform a **New and Complete** installation, not a **Preservation** installation.

**Note:** Do not install any fix levels at this time. You will do this later in the installation process.

- Make sure that the machine’s language locale is set to the language in which you plan to run Trust Authority applications.
- Trust Authority supports the AIX Trusted Computing Base (TCB). If you want to use this feature, which further extends the security of your operating system, select the option to enable it when installing AIX.
- When configuring TCP/IP, enter the system short name as the HOSTNAME. For example, enter 'hostname' instead of 'hostname.mycompany.com'. To verify you have done this correctly, complete the following steps:
  1. Type smitty.
  2. Select: **Communications Applications and Services**.
  3. Select: **TCP/IP**.
  4. Select: **Minimum Configuration and Startup**.
  5. Select the appropriate network interface from the **Available Network Interfaces** list. For example, select: **en0 Standard Ethernet Network Interface**.
  6. Verify the HOSTNAME value is in the correct form.

**Verify filesets**

After installing AIX and restarting the system, confirm that the following filesets were installed:

<table>
<thead>
<tr>
<th>Fileset Name</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bos.adt.prof</td>
<td>4.3.3.3</td>
<td>Java Runtime Edition Profs</td>
</tr>
<tr>
<td>X11.adt.motif</td>
<td>4.3.3.1</td>
<td>Java Runtime Edition Motifs</td>
</tr>
<tr>
<td>X11.applets.aixterm</td>
<td>4.3.3.0</td>
<td>AIXwindows aixterm Application</td>
</tr>
<tr>
<td>X11.applets.rte</td>
<td>4.3.3.0</td>
<td>AIXwindows Runtime Configuration Applications</td>
</tr>
<tr>
<td>X11.applets.util</td>
<td>4.3.3.0</td>
<td>AIXwindows Utility Applications</td>
</tr>
<tr>
<td>X11.base.l1ib</td>
<td>4.3.3.0</td>
<td>AIXwindows Runtime Libraries</td>
</tr>
<tr>
<td>X11.base.rte</td>
<td>4.3.3.0</td>
<td>AIXwindows Runtime Environment</td>
</tr>
<tr>
<td>X11.base.smt</td>
<td>4.3.3.0</td>
<td>AIXwindows Runtime Shared Memory Transport</td>
</tr>
<tr>
<td>X11.compat.l1ib.X11R5</td>
<td>4.3.3.0</td>
<td>AIXwindows X11R5 Compatibility Libraries</td>
</tr>
<tr>
<td>X11.fnt.defaultfonts</td>
<td>4.3.3.0</td>
<td>AIXwindows Default Fonts</td>
</tr>
<tr>
<td>X11.motif.lib</td>
<td>4.3.3.0</td>
<td>AIXwindows Motif Libraries</td>
</tr>
<tr>
<td>X11.motif.mwm</td>
<td>4.3.3.0</td>
<td>AIXwindows Motif Window Manager</td>
</tr>
<tr>
<td>ifor ls.base.cli</td>
<td>4.3.3.0</td>
<td>License Use Management Runtime Code</td>
</tr>
<tr>
<td>ifor ls.base.gui</td>
<td>4.3.3.0</td>
<td>License Use Management Runtime GUI</td>
</tr>
<tr>
<td>ifor ls.client.base</td>
<td>4.3.3.0</td>
<td>License Use Management Client Runtime</td>
</tr>
<tr>
<td>ifor ls.client.gui</td>
<td>4.3.3.0</td>
<td>License Use Management Client GUI</td>
</tr>
<tr>
<td>ifor ls.compat.cli</td>
<td>4.3.3.0</td>
<td>License Use Management Compatibility Code</td>
</tr>
</tbody>
</table>
If all of these filesets were not installed, install them before proceeding with the installation.

**Verify adequate paging spaces**

There must be at least 512 MB of paging spaces. To verify that there is adequate paging spaces, complete the following steps:

1. Type `smitty`.
2. Select: *System Storage Management (Physical & Logical Storage)*.
3. Select: *Logical Volume Manager*.
4. Select: *Paging Space*.
5. Select: *List All Paging Spaces*.
6. If the total size is not 512MB or more, complete the following steps:
   a. Press F3 or Cancel.
   b. Select: *Change/Show Characteristics of a Paging Space*.
   c. Select the paging space name you want to increase.
   d. Add the number of additional 4MB partitions needed to have 512MB of paging space.

**Apply the fix level to AIX**

After you have verified the fileset for AIX, you need to install fix level ML 4330–02. Obtain the AIX fix level ML 4330–02 patch and install it according to the accompanying documentation.

**Set up AIX disk partitions**

Using the AIX System Management Interface Tool (SMIT), set up the following disk partitions. This suggested configuration is based on using two disk drives with 4.5 GB of usable space for the rootvg and datavg partitions.

**Note:** This discussion assumes that all the server components are being installed on the same machine. If you install the Certificate Authority and Audit subsystem on a machine that is separate from the Registration Authority server, adjust the procedure accordingly.

- For the rootvg partition:
  - Set the root (/) partition to 64 MB (128,000 512-byte blocks).
  - Set the /usr partition to 3 GB (6,000,000 512-byte blocks).
  - Set the /tmp partition to 200 MB (400,000 512-byte blocks).
  - Set the /var partition to 500 MB (1,000,000 512-byte blocks).
  - Set the /home partition to 200 MB (400,000 512-byte blocks).

- For the datavg partition:
  - Create a /local partition and set it to 2 GB (4,000,000 512-byte blocks).
  - Create a /dbfsibm partition and set it to 500 MB (1,000,000 512-byte blocks).
This is the default file system for the Trust Authority CA. Note that the size may need to be adjusted in accordance with the number of certificates that are issued.

- Create a /dbfspkrf partition and set it to 300 MB (600,000 512-byte blocks).
  This is the default file system for the registration facility. Note that the size may need to be adjusted in accordance with the number of users who register for certificates.

- Create a /dbfsadt partition and set it to 300 MB (600,000 512-byte blocks).
  This is the default file system for the Audit subsystem. Note that the size may need to be adjusted in accordance with the number of audit events that are logged.

- Create a /dbfskrb partition and set it to 300 MB (600,000 512-byte blocks).
  This is the default file system for the key backup/recovery facility.

**Note:** The size may need to be adjusted in accordance with the number of key backup requests that are issued.

**Create a CD-ROM filesystem**

To install Trust Authority and its prerequisite products, you must have a CD-ROM filesystem mounted as /cdrom. If necessary, use the following command to create a definition for this filesystem:

```
crfs -v cdrfs -d /dev/cd0 -m /cdrom -p ro -A no
```

Alternatively, you can use SMIT to create it:

```
smitty crcdrfs
```

**Change the number of AIX system users**

Enter the following command to change the number of AIX system users. You must restart the system for this command to take effect.

```
chlicense -u 100
```

**Ensure host name resolution**

Follow the steps below to set up AIX so that your local server can correctly resolve host names.

1. Create a file in the /etc directory named `netsvc.conf` that contains only the following line (note that there are no spaces in this statement):
   ```
   hosts=local,bind4
   ```
   You can create this file by using a text editor such as vi, or by entering the following command:
   ```
   echo hosts=local,bind4 > netsvc.conf
   ```

2. Edit the `/etc/hosts` file and ensure this file references the server you are setting up. For example:
   ```
   127.0.0.1 loopback localhost
   192.40.168.20 taserver.company.com taserver
   ```
   The second line in the preceding example identifies the IP address, fully qualified host name, and short host name of the AIX server you are setting up.

3. Create or modify the `/etc/resolv.conf` file to include only the following lines:
   ```
   domain company.com
   nameserver 10.10.10.90
   ```
The first line in the preceding example identifies the domain name of the server you are setting up. The second line identifies the IP address of the DNS name server.

**Create a system image**

Although not required, IBM recommends that you back up your AIX system configuration before proceeding with the installation of Trust Authority. Having a backup image enables you to restore the system in the event that problems occur.

To create a system image, enter the following commands as root and select your preferred options:

```
smitty mksysb
smitty savevg
```

**Installing the database software**

Trust Authority uses IBM DB2 Universal Database software to manage data. The IBM DB2 Universal Database software is provided with the IBM WebSphere Application Server Standard Edition version 3.5.0 product. The IBM DB2 Universal Database software provided with IBM WebSphere Application Server is intended solely for use by Trust Authority applications. If you want to customize the database software, or use it for purposes other than Trust Authority, you must purchase a license for a complete version of IBM DB2 Enterprise Edition, version 6.1.

The following sections provide procedures for installing the base database software and for installing a software upgrades for the database, xLC runtime code, and the JDK. If you are setting up Trust Authority in a multiple machine configuration, you must install these programs on each machine where you plan to install a Trust Authority server component. Note the following guidelines:

- During configuration, Trust Authority automatically creates the databases that are required by the server programs. Unless it already exists, it also creates a database for the Directory.
- Before installing Trust Authority, you must ensure that the required version of database software is installed on each machine where you plan to install a Trust Authority server component. You must ensure that the database system is functioning correctly on its own before you install Trust Authority.
- After installing the database software, be sure to restart the system. You must ensure that environment variables are set correctly before you install the Trust Authority or Directory server software.

**Install DB2**

Use the following procedure to install the base database software.

1. Log in as root.

2. Place `WebSphere Application Server IBM SecureWay Directory Disk` in the CD-ROM drive. Enter the following command to mount the CD-ROM:

```
mount /cdrom
```

3. Change to the `db2` directory on the CD: `/cdrom/Db2`.

4. Enter the following command to run the database installation script:

```
./db2setup
```
During installation, the program checks to see whether a previous version of DB2 exists on the system and whether the machine has adequate disk space. If DB2 already exists, the software is upgraded to the required level during installation. If there is not enough space, the /usr file system is increased to 400 MB free space.

5. Select: **DB2 UDB Enterprise Edition**.

6. Select: **DB2 Product Messages**.

7. Select the appropriate language for your area and then select: **OK**.

8. Select: **DB2 Product Library**.

9. At Create DB2 Services, select: **OK**.

10. Select: **Create DB2 Instance**.

11. Set UserName to `db2inst1` and Home Directory to `/home/db2inst1`. Leave all other values set to their default.

12. Enter values for **Password** and **Verify Password**.

13. Select: **Properties**.

14. For the Authentication Type, select: **Client**.

15. Select: **OK**.

16. Select: **OK**.

17. For Authentication, enter values for **Password** and **Verify Password**.

18. Select: **OK**.

19. Select: **OK**.

20. Select: **OK**.

21. Select: **Continue**.

22. Select: **OK**.

23. Select: **OK**.

24. Select: **OK** to exit or view log.

25. Select: **Close**.

26. Select: **OK**.

27. Select: **OK**.

28. Change directories to `/usr/lpp/db2_06_01/cfg`.

29. Enter the following command:

    ```
    ./db2ln
    ```

30. If you are going to continue to install the prerequisites for Trust Authority, skip this step. Otherwise, after the software is installed, enter the following command to unmount the Trust Authority media. No process can be accessing any portion of the /cdrom tree when you run this command.

    ```
    umount /cdrom
    ```
Installing SecureWay Directory

Trust Authority uses the IBM SecureWay Directory to store and maintain information about certificates issued through the registration facility. Use the procedures in the following sections to install and set up the Directory software. You can install this software on a remote machine or on the same machine where you plan to install a Trust Authority server component.

Install Directory software

1. Log in as root.
2. Place the Directory Server version 3.1.1 CD into the system’s CD-ROM drive. Enter the following command to mount the CD-ROM:
   ```
   mount /cdrom/ldap311_us
   ```
3. Change to the /cdrom/usr/sys/inst.images directory and enter the following command:
   ```
   smitty install_all
   ```
4. Select . (period) for the INPUT device / directory for software option.
5. At Install and Update from ALL Available Software, press F4 and then use F7 to select the following components to install:
   ```
   ldap.client ALL
   + 3.1.1.1 SecureWay Directory Client Runtime (No Encryption)
   + 3.1.1.1 SecureWay Directory Client SDK
   
   ldap.html.en_US ALL
   + 3.1.1.0 SecureWay Directory Install/Config Gd - U.S. English
   + 3.1.1.0 SecureWay Directory Man Pages - U.S. English
   
   ldap.msg.en_US ALL
   + 3.1.1.0 SecureWay Directory Messages - U.S. English
   
   ldap.server ALL
   + 3.1.1.1 SecureWay Directory Server Administrative Interface
   + 3.1.1.1 SecureWay Directory Server Framework
   + 3.1.1.1 SecureWay Directory Server Runtime (No Encryption)
   ```
6. Enter the following command to unmount the Directory media. No process can be accessing any portion of the /cdrom tree when you run this command.
   ```
   umount /cdrom
   ```

Note: In a multiple machine configuration, each Trust Authority server must have the Directory client software installed before you run the Trust Authority configuration applet. To install this software, you must install the ldap.client option from the SecureWay Directory Server CD-ROM on each machine except the one where you just installed the Directory server software. The critical file that must be installed on each machine is libldap.a.

Use the Directory with Trust Authority

Before you install or configure the Trust Authority server components, you need to understand how Trust Authority interacts with the Directory. To learn about Directory schema requirements and how to configure the Directory for Trust Authority, read "Using the SecureWay Directory With Trust Authority." This document is available at the Trust Authority Web site.
Upgrade Java

The version of Java on the system needs to be updated to a more recent version. To update Java, complete the following steps:

1. Log in as root.
2. If the Tivoli SecureWay PKI for AIX CD is not mounted, do so.
3. Change the directory to the following: /cdrom/aix/Java_1.2.2.ptf8.
4. Enter the following command:
   ```bash
   smitty install_latest
   ```
5. Select "period" in INPUT device / directory for software.
6. Press the PF4 key.
7. Select the following filesets:
   ```
   Java_dev2.rte
   Java_dev2.adt
   ```
8. Press Enter.
9. If you are going to continue to install the prerequisites for Trust Authority, skip this step. Otherwise, after the software is installed, enter the following command to unmount the Trust Authority media. No process can be accessing any portion of the /cdrom tree when you run this command.
   ```bash
   umount /cdrom
   ```

Create the WebSphere Application Server database

Before you install WebSphere Application Server, you must create a DB2 database for it. To create a database, complete the following steps:

1. Log in as root.
2. Enter the following command:
   ```bash
   su - db2inst1
   ```
3. Start the DB2 console using the following command:
   ```bash
   db2
   ```
4. Start DB2 by entering: `db2start`.
5. Create and configure the database for WebSphere Application Server by entering the following two commands:
   ```
   create database was_db
   update db cfg for was_db using applheapsz 256
   ```
6. Exit the DB2 console by entering: `quit`.
7. Stop DB2 by entering: `db2stop`.
8. Start DB2 by entering: `db2start`.
9. Enter the following command: `exit`. 
Installing the Web server software

Trust Authority uses the IBM WebSphere Application Server and IBM HTTP Server to support its Web-based functions. To ensure that the Web server programs are installed correctly for use with Trust Authority, follow this procedure to install the software on an AIX platform. You must install the software on the machine where you plan to install the Registration Authority component.

Note that even though WebSphere has an administrative interface for managing servlets, it is neither possible nor necessary to use it to manage Trust Authority servlets.

After you install Trust Authority, a post-installation program updates the Web server with information that is required by Trust Authority. When you start the Web server, it uses the configuration file that Trust Authority created for this purpose.

Note: Be sure to review the discussion of how Trust Authority configures ports on the Web server in "Configuring IP aliases for the Web server" on page 23. If you want to configure ports differently, you must do so before you configure Trust Authority.

Install WebSphere Application Server

1. Log in as root.
2. Place WebSphere Application Server IBM SecureWay Diirectory Disk in the CD-ROM drive. Enter the following command to mount the CD-ROM:
   ```
   mount /cdrom
   ```
3. You must install WebSphere in a graphical X11 environment. Enter the following command to export the proper DISPLAY environment variable for the WebSphere installation program to open, where `yourhost:0.0` is the proper value for your system:
   ```
   export DISPLAY=yourhost:0.0
   ```
4. Install WebSphere:
   a. Change to the `/cdrom/aix` directory.
   b. Enter the following command to run the install.sh script. Preferably, install this software in `/usr/WebSphere/AppServer`.
      ```
      ./install.sh
      ```
   c. On the Welcome window, click Next.
   d. On the Install Options window, select Custom installation and click Next.
   e. On the Choose Destination Location window, accept the default location and click Next.
   f. On the Choose Application Server Components window, select all components and click Next.
   g. On the Choose Application Server Components window, select IBM HTTP Sever plug-in and click Next.
   h. On the Database Options window, select DB2 from the database Type drop-down list and fill in the following fields as listed:
      ```
      Database Name: was_db
      DB Home: /home/db2inst1
      Database User ID: db2inst1
      Database Password: yourpassword Confirm Password: yourpassword
      ```
i. Click **Next**.

j. On the Security Information window, enter the password for the root ID and click **Next**.

k. On the Select Destination Directory window, click **Next**.

l. On the Install Options Selected window, click **Next**.

m. On the next window, click **OK** to begin installing the product.

5. If you are going to continue to install the prerequisites for Trust Authority, skip this step. Otherwise, after the software is installed, enter the following command to umount the Trust Authority media. No process can be accessing any portion of the /cdrom tree when you run this command.

   ```
   umount /cdrom
   ```

**Set up IP aliases**

"Configuring IP aliases for the Web server" on page 24 contains a discussion of how Trust Authority configures ports on the Web server to process secure and non-secure transactions. If you want to use a different configuration, use IP aliases to define those ports.

**Note:** Before you run the Setup Wizard, you should run the hostname command. Make sure that the values you plan to use for the host names of the Trust Authority server components match the output of the hostname command.

If the output of the hostname command is not the one that you want users to specify when accessing the registration facility through the browser enrollment facility, you need to change the TCP/IP settings on the server. For example:

1. Enter: `# smitty tcpip`

2. Select **Minimum Configuration & Startup**.

3. Select **Token ring Network Interface**.

4. Change the **HOSTNAME** field to the host name you want to use.

5. To verify the changes, enter: `# hostname`

   When you run the Setup Wizard to configure Trust Authority, the host names you specify for the various Trust Authority servers must match the host name you specified in the preceding procedure.

**Upgrade GSKIT**

The version of GSKIT installed by WebSphere Application Server needs to be upgraded to a more recent version. To do this, complete the following steps:

1. Log in as root.

2. Place the **Tivoli SecureWay PKI for AIX** cd into the system’s CD-ROM drive.

3. If the CD-ROM drive is not already mounted, do so.


5. Enter the following command: `smitty install_latest`.

6. Select "." (period) for the INPUT device / directory for software option.

7. At Install and Update from LATEST Available Software, press Enter.
8. If you are continuing to install the prerequisites for Trust Authority, you can skip this step. Otherwise, unmount the CD-ROM drive.

**Upgrade IBM HTTP Server**

1. Log in as root.
2. Place the *Tivoli SecureWay PKI for AIX* CD into the system’s CD-ROM drive.
3. If you have not already mounted the CD-ROM drive, do so.
4. Change to the `/cdrom/aix/HTTP-1.3.12.1` directory.
5. Enter the following command to install IBM HTTP Server (IHS) 1.3.12.1:
   ```bash
   smitty install_latest
   ```
6. Select "." (period) for the INPUT device / directory for software option.
7. At Install and Update from LATEST Available Software, press Enter.
8. If you are continuing to install the prerequisites for Trust Authority, you can skip this step. Otherwise, unmount the CD-ROM drive.

**Note:** After the Web server software has been installed and upgraded, you must disable the automatic startup feature of the IBM HTTP Server service. To do this, complete the following steps as root. (You may receive messages about the subsystem not being active. If so, you can ignore the messages.)

1. Change to the `/etc` directory.
2. Edit the file `inittab` and delete the entry for `ihshttpd`.
3. Stop the IBM HTTP Server service that WebSphere may have already started. To do so, complete the following steps:
   a. List the possible processes: `ps -ef | grep http`.
   b. Identify the process `/usr/HTTPServer/bin/httpd`.
   c. Find the parent process ID (the third field from the left).
   d. If the parent process ID is not equal to 1, kill the parent process by entering the `kill` command.
   e. Enter the following command: `slibclean`.

You must also change the version of Java that WebSphere uses by default, to the more current version that has been installed. To do this, Perform these commands:

```bash
cd /usr/WebSphere/AppServer
mv java java.old
ln -s /usr/java_dev2 java
```

**Start WebSphere Application Server**

Before you install Trust Authority, you must start WebSphere Application Server. To start WebSphere Application Server, complete the following steps:

1. Change directories to `/usr/WebSphere/AppServer/bin`.
2. Run the following command: `./startupServer.sh &`
3. Change directories to `/usr/WebSphere/AppServer/logs`.
4. Watch the trace file by entering the following command: `tail -f tracefile` When you see the message, “A WebSphere Administration Server open for e-business,” WebSphere Application Server will be started.

5. Press Ctrl + C to exit the tail command.

**Installing the 4758 coprocessor**

You must decide whether you want to use the IBM 4758 cryptographic card to protect CA signing keys. If so, you must install the 4758 hardware and its cryptographic support program on the server where you plan to install the Certificate Authority.

For information about installing and setting up the 4758 coprocessor, see "Using the SecureWay 4758 Coprocessor With Trust Authority". This document is available at the IBM SecureWay Trust Authority Web site.

**Installing Trust Authority**

Before you begin installing Trust Authority, be sure to read the latest version of the product Readme file. To obtain the most current version of this file, access the Trust Authority Web site.

Use the following guidelines to install the Trust Authority product components.

- You must install all the server programs on the same platform, in this case AIX.
- If you previously installed IBM KeyWorks version 1.1.1, you must either install Trust Authority on a different machine, or remove the KeyWorks software and any associated applications before you start the Trust Authority installation program.
- If you are setting up Trust Authority in a multiple machine configuration, you must repeat the installation procedures until you have installed all server components on the intended machines.
- When you install the Client application or the RA Desktop applet, you first install an installation image. You must then distribute the image or make it available on your network so that users can run the installation program from a local Windows machine. For instructions on how to install, configure, and uninstall these programs, see the following documents:
  - Trust Authority User’s Guide
  - Trust Authority RA Desktop Guide
- If you did not restart the system after installing the prerequisite software, do so now. You must ensure that environment variables are correct before you install Trust Authority.
- Use PING or another network connectivity tool to verify that host names and IP addresses are valid and known to your network’s DNS server.

**Install KeyWorks**

To install KeyWorks, complete the following steps:

1. Log in as root.
2. Place the Tivoli SecureWay PKI for AIX CD into the system’s CD-ROM drive.
3. If you have not already mounted the CD-ROM drive, do so.
4. Change to the `/cdrom/aix/kw` directory.

5. Enter the following command to install KeyWorks:
   ```
   smitty install_all
   ```

6. Select "." (period) for the INPUT device / directory for software option.

7. At Install and Update from LATEST Available Software, press Enter.

8. If you are continuing to install Trust Authority, you can skip this step. Otherwise, unmount the CD-ROM drive.

### Install the server software

1. Log in as root.

2. Place *Tivoli SecureWay PKI for AIX* in the CD-ROM drive. Enter the following command to mount the CD-ROM:
   ```
   mount /cdrom
   ```

3. Use SMIT to install the software:
   a. Select **Software Installation and Maintenance**.
   b. Select **Install and Update Software**.
   c. Select **Install and Update from Latest Available Software**.
   d. At **INPUT device/directory for software**, in the **Entry Fields** area, type the fully qualified path to the CD-ROM drive and press **Enter**.

   **Note:** Be sure to specify the device name (such as `/dev/cd0`) or the full path to the mounted CD-ROM directory (such as `/cdrom/usr/sys/inst.images`). You cannot install software from the Trust Authority CD-ROM by mounting it, setting the current directory to be on the CD, and attempting to install from path ".".

e. At **SOFTWARE to install**, press the **F4** key to view a list of the filesets available for installation.

f. Using the following table as a guideline, select the component or components you want to install on this machine, and press **Enter**.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Authority and Registration Authority server</td>
<td>Installs the main Trust Authority programs and the Registration Authority server software, including all files needed for the registration facility.</td>
</tr>
<tr>
<td>Certificate Authority and Audit server</td>
<td>Installs the Certificate Authority and Audit subsystem programs.</td>
</tr>
<tr>
<td>Directory server</td>
<td>Installs software that the Trust Authority components need to interact with the Directory.</td>
</tr>
<tr>
<td>Trust Authority Client</td>
<td>Installs an installation image for the Trust Authority Client application. (Windows NT only)</td>
</tr>
<tr>
<td>Registration Authority Desktop</td>
<td>Installs an installation image for the Trust Authority RA Desktop applet. (Windows NT only)</td>
</tr>
</tbody>
</table>
Change bootstrap values

Use this procedure only if you want to change any of the default configuration values — values that you cannot change when running the configuration applet or after the system has been configured. You must make all bootstrap changes before you run the Trust Authority post-installation configuration program.

Trust Authority runs a bootstrap program as part of the post-installation process. Input to the bootstrap program is an SQL script named createconfig_start.sql that loads the configuration database with default values and creates database table definitions in the ConfigDataTbl database table. This table contains the system configuration data for all the Trust Authority components. Several values in this SQL script cannot be changed once the configuration process has started.

Note: Under critical circumstances where a default value may cause a problem in your operating environment, you can also change Trust Authority template files prior to configuration. For more information, contact your IBM support representative.

To change a bootstrap value, edit the createconfig_start.sql file. The default location for this file is /usr/lpp/iau/bin.

Use the following table as guidelines when making any changes:

- To change the value for DATABASE PATHNAME, you must specify the entire path to the new location. For example: /local/dbfsibm.
- The distinguished names (DNs) for the Trust Authority RA, Directory administrator, and Audit subsystem are transparent to the user. If you want to change them, be sure to change only the common name (CN) attribute. The CA DN base you specify during configuration will be applied to the CN you select.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS_RO_KEYSIZE</td>
<td>Web server keyring key size. Options 0-3, as defined in the KeySize enumeration, are as follows:</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>■ 0 = 512</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 1 = 768</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 2 = 1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ 3 = 2048</td>
<td></td>
</tr>
<tr>
<td>DATABASE_PATHNAME</td>
<td>Fully qualified path for where the CA database instance physically resides (the CA component).</td>
<td>dbfsibm</td>
</tr>
<tr>
<td>DATABASE_PATHNAME</td>
<td>Fully qualified path for where the Audit database instance physically resides (Audit subsystem component).</td>
<td>dbfsadt</td>
</tr>
<tr>
<td>DATABASE_PATHNAME</td>
<td>Fully qualified path for where the registration database instance physically resides (RA component).</td>
<td>dbfspkrf</td>
</tr>
</tbody>
</table>
Run the post-installation configuration program

After you install the Trust Authority server software, you must run a post-installation configuration program, CfgPostInstall. You must run this program before you run the Setup Wizard to configure Trust Authority.

This program creates a Web server configuration file (httpd.conf) that allows the Web server to be started with parameters required by Trust Authority. It also prepares the Web server to run the configuration applet, creates a Trust Authority configuration user account (cfguser), creates the configuration database, and populates the database with default configuration data.
To run the post-installation configuration program, log in as root, change to the bin subdirectory, and run CfgPostInstall. For example:

```
# su - root
# cd /usr/lpp/iau/bin
# ./CfgPostInstall
```

CfgPostInstall prompts you to set and confirm the cfguser account password and then prompts you to set and confirm the Control Program password. The password for cfguser controls access to the cfguser account and to the CfgApplet wizard page. The password for the Control Program restricts access to the Control Program. It is recommended that the password for the Control Program be different than the password for cfguser. The cfguser password you create must be a valid system password, not to exceed eight characters in length.

CfgPostInstall also prompts you to select the instance of DB2 you want to use. A list will show all possible instances of DB2 available. You should select the instance you created when installing DB2 for Trust Authority. For example, db2inst1.

**Post-installation checklist**

Use the following checklist to make sure that you are ready to begin configuring Trust Authority. For information about running the Setup Wizard, see the Trust Authority Configuration Guide.

1. Log in as root, and enter the following commands to create a backup system image:
   ```
   smitty mksysb
   smitty savevg
   ```
2. To aid in future problem resolution, create a list of all the software that is installed on each server. Log in as root, and enter the following command:
   ```
   # lslpp -al > tmp/sys_software.txt
   ```
3. If you do not intend to use the default configuration values for the Web server ports, you must configure the IP aliases before you run the Setup Wizard. The configuration programs rely on these values when creating the CA certificate for your system. See "Configuring IP aliases for the Web server" on page 24 for a discussion of how Trust Authority configures and uses ports on the Web server for secure and non-secure transactions.
4. Decide on the distinguished names you want to use for the Trust Authority CA and its agents, the Directory administrator and the Directory root. These DNs must be unique. If necessary, review the guidelines in "Using the SecureWay Directory With Trust Authority" to make sure that the DNs for these objects support your intended certification hierarchy. This document is available on the Trust Authority Web site.
5. Print the Trust Authority Configuration Data Form to become familiar with information you must have on hand before you configure the system. Use the form to record information about your system, such as your server host names and your preferred distinguished names.

   The configuration data form is available at the Trust Authority Web site.

**Run the backup utility**

The Trust Authority backup utility, ta-backup, is a tool for saving configuration data that is not stored in any of the DB2 databases. The ancillary file data such as file permissions are also saved. Use DB2 utilities for backing up DB2 databases.
The backup utility accepts one parameter that identifies the directory where backup data is to be written. This backup directory is the root directory to be used for saving all data files. To avoid name conflicts within the backup directory, the backup utility saves files with the same directory structure as exists on the system being saved.

The following example illustrates the program syntax:

```
ta-backup -d backup_directory
```

where:

- `.backup_directory` is the directory to be used for data backup. The default path is `/usr/lpp/iau/backup`.

Follow these steps to run the ta-backup utility offline:

1. Log in as root.
2. Optionally create the directory to which you want to back up Trust Authority configuration data. For example:
   ```
   mkdir /usr/lpp/iau/my_tabackup
   ```
3. Change to the Trust Authority bin directory. The default path is `/usr/lpp/iau/bin`.
4. Enter the following command and specify the absolute path to where you want data to be backed up:
   ```
   ta-backup -d /usr/lpp/iau/my_tabackup
   ```
This chapter provides procedures for installing Trust Authority and its prerequisite products on a Windows NT platform.

**Note:** Trust Authority version 3.7.0 does not support Windows NT. This information has been included as a reference only.

Before you begin installing software for Trust Authority, be sure to read the latest version of the product *Readme* file. To obtain the most current version of this file, access the IBM SecureWay Trust Authority Web site.

**Note:** The main procedures in this chapter assume that you are installing Trust Authority for the first time. If you are migrating from a previous version of the product, you should back up the data files before beginning the installation. Refer to the instructions in “Run the backup utility” on page 60. Following the backup, run CfgUnInstall from the command line and then proceed with the Trust Authority installation.

IBM recommends that you install software for Trust Authority in the following order:

1. Microsoft Windows NT operating system version 4.0 with Service Pack 5
2. Trust Authority database software (IBM DB2 Universal Database for Trust Authority)
3. Sun Java Development Kit (JDK) version 1.1.6 or greater
4. IBM HTTP Server (IHS) version 1.3.3.1, including the Global Services Kit (GSK)
5. IBM WebSphere Application Server version 2.0.3.1
7. Trust Authority server software, which includes the core server programs and installation images for the Client application and RA Desktop.

**Multiple Machine Configuration**

If you are not installing all the server software on the same machine, you must repeat the procedures below to install Windows NT and the Trust Authority database software on each component machine.
Setting up Windows NT

Use the following guidelines when installing Windows NT software on the machine or machines where you plan to install Trust Authority software. If you previously installed NT, use these guidelines as a checklist to make sure that you installed all the files that are required by the Trust Authority components.

If you are setting up Trust Authority in a multiple machine configuration, you must install NT on each machine where you plan to install a Trust Authority server component.

- When installing Windows NT, you must install the TCP/IP Protocol. You cannot use DHCP unless you have a dynamic DNS server.

- Use the following guidelines to enable connectivity:
  - Ensure that IP addresses and host names are allocated and fixed.
  - Ensure that you have IP connectivity. For example, test your ability to PING another machine.
  - Ensure that DNS and reverse DNS are operating correctly. For example, ensure that the command `ping hostname` resolves to the correct IP address and that the command `ping -a IPaddress` resolves to the correct host name.

- Ensure that the machine has a temp directory. If it does not exist, create it. To check for or to create the temp directory, enter the command `md %temp%`. If the directory exists, the system displays the message "A subdirectory or file drive:\TEMP already exists". Otherwise, the system creates the temp directory.

- Set the machine’s virtual memory to at least 400 MB:
  1. Select **Start** → **Settings** → **Control Panel**.
  2. Double-click **System**, and select the **Performance** tab.
  3. In the **Virtual Memory** area, click **Change**.
  4. Change the **Initial Size** value to 400 MB and **Maximum Size** to 500 MB.
  5. Click **Set** then **OK** to close the dialog box.
  6. Click **OK** to close the System Properties window.
  7. Click **Yes** to the prompt to restart your computer.

- Create a Windows NT user that serves as the Trust Authority configuration user. The configuration programs use this username and password to create the required databases and configure the system. Use the Windows NT Administrative Tools to set up this user as follows:
  1. From the Administrative Tools program group, run **User Manager**
  2. Add the account **cfguser** by copying the Administrator account (highlight the Administrator entry and press the F8 key). The user must have Windows NT Administrator privileges.
  3. Type a password for cfguser, type the same password again to confirm it, deselect **User Must Change Password At Next Logon**, and click **OK**. The password assigned to this username must be exactly eight characters long. To optimize security, you should specify a string that does not spell a real word. The password should also use a mix of uppercase and lowercase characters and include at least one number.
Be sure to remember this username and password. You will need to specify it when installing and configuring the system, and it may be needed to run certain Trust Authority system administration tools.

If you plan to install Trust Authority in a multiple machine configuration, be sure to create the same username and password on each machine.

IBM recommends that you back up your Windows NT system before proceeding with the installation of Trust Authority. Having a backup image will enable you to restore the system in the event that problems occur. You can use the Backup program provided by the Windows NT Administrative Tools to create a system image. Alternatively, use another Windows-compliant backup program of your choice.

**Installing the database software**

Trust Authority uses IBM DB2 Universal Database software to manage data. The software provided with Trust Authority is intended solely for use by Trust Authority applications. If you want to customize the database software, or use it for purposes other than Trust Authority, you must purchase a license for a complete version of IBM DB2 Enterprise Edition, version 5.2, and apply fix pack 10.

Use the following procedure to install the database software. If you are setting up Trust Authority in a multiple machine configuration, you must install the Trust Authority database software on each machine where you plan to install a Trust Authority server component.

1. Place *IBM SecureWay Trust Authority for NT, Disk 1* in a CD-ROM drive.
2. Select Start → Run, click Browse to change to the CD-ROM drive, and run setup.exe.
3. On the Choose Setup Language window, select a language for this installation and click OK.
4. Review the information on the Welcome window and click Next.

   **Note:** If DB2 already exists on this machine and is at the correct level, the program advances to the Setup Complete window. At that point, click Finish to complete the installation.

5. On the Choose Destination Location window, click Next to use the default installation path, or select the drive and destination folder where you want to install the software and then click Next. (The default path, c:\Program Files\IBM\Trust Authority, should be acceptable.)
6. On the Specify Database Administrator window, type a Username and Password for the database administrator, re-type the password to confirm it, and click Next. The suggested value is db2admin for both entries.
7. The program begins installing the database software. Be patient; the process may take several minutes.
8. On the Setup Complete window, click Finish to complete the installation.
Installing the Web server software

Trust Authority uses the IBM WebSphere Application Server and IBM HTTP Server to support its Web-based functions. To ensure that the Web server programs are installed correctly for use with Trust Authority, follow this procedure to install the software on a Windows NT platform. You must install the software on the machine where you plan to install the Registration Authority component.

Trust Authority includes an updated version of the WebSphere Application Server on the Trust Authority for AIX and NT Disk 2 CD-ROM. You use the WebSphere Application Server version 2.02 CD-ROM to install the IBM HTTP Server, and the Trust Authority CD-ROM to install the WebSphere Application Server.

Note that even though WebSphere has an administrative interface for managing servlets, it is neither possible nor necessary to use it to manage Trust Authority servlets.

Install the JDK

1. Insert the WebSphere Application Server version 2.0.2 CD in the CD-ROM drive.
2. Change to the \NT\jdk directory, and run the JDK setup.exe program.
3. On the Welcome window, click Next.
4. On the Software License Agreement window, read the agreement and click Yes to accept it.
5. On the Select Components window, accept the default selections (Program Files, Library and Header Files, and Demo Applets). Click Next to use the default installation path, or select the drive and destination folder where you want to install the JDK and then click Next. (The default path should be acceptable.)
6. On the Start Copying Files window, review the choices you made and click Next to proceed.
7. On the Setup Complete window, click Finish.
8. When the Readme file is displayed, review it and then close it (click the X in the upper right-hand corner of the window).

Install IBM HTTP Server

1. Insert the WebSphere Application Server version 2.0.2 CD in the CD-ROM drive.
2. Change to the \NT\httpd directory, and run the IHS setup.exe program.
3. On the Welcome window, click Next.
4. On the Software License Agreement window, read the agreement and click Yes to accept it.
5. On the Choose Destination Location window, click Next to use the default installation path, or select the drive and destination folder where you want to install the HTTP Server and then click Next. (The default path should be acceptable.)
6. On the Setup Type window, select Custom and click Next.
7. On the Select Components window, there are two panes: the left side lists the names of the component sets; the right side lists the components that make up a given component set. Select Base on the left and deselect Apache Source on the right. If you do not want to install the Documentation, deselect it as well. Click Next to continue.
8. On the Select Program Folder menu, click **Next** to accept the default program folder, or type the folder name you want to use and then click **Next**.

9. On the Information for Service Setup window, type **cfguser** for the **User ID**, type the password you created for this account, confirm the password, and then click **Next**.

10. On the Setup Complete window, you have a choice to reboot now or later. Choose later (**No**) and then click **Finish**.

**Note:** After installing the IBM HTTP Server, you must set the server service to manual so that the server does not start as a service. To do this:

1. Select **Start** → **Settings** → **Control Panel**.
2. Double-click **Services** and select the **IBM HTTP Server** service.
   - Click **Stop** (if it has already been started).
   - Click **Startup**, and change the **Startup Type** to **Manual**.
   - Click **OK**.
   - Click **Close**, and exit the Control Panel.

### Install WebSphere Application Server

1. Place *IBM SecureWay Trust Authority for AIX and NT Disk 2* in the CD-ROM drive.

2. Change to the \WinNT\WebSphereAS-2031 directory, and run the was2031.exe program.

3. On the WebSphere Application Server window, click **Next**. (You can ignore the warning about stopping the HTTP Server.)

4. On the Choose Target Directory window, click **Next** to accept the default installation path, or select the drive and destination folder where you want to install the software and then click **Next**.

5. On the Choose Application Server Components window, you can optionally deselect **Documentation** and **Samples**; all other components are required. Click **Next** to proceed.

6. On the Select Java Development Kit or Runtime Environment window, make sure that **Java Development Kit 1.1.6** is selected, and then click **Next**.

7. On the Choose Application Server Plugins window, click the box for **IBM HTTP Server Version 1.3.3.x** and then click **Next**.

8. On the Select Program Folder window, click **Next** to accept the default program folder, or type the folder name you want to use and then click **Next**.

9. On the Configure IBM HTTP Server window, make sure that it displays the correct path for the location of your installed IBM HTTP Server \conf directory, and then click **OK**.

10. On the Setup Complete window, click **Finish**.

11. When the Readme file is displayed, review it and then close it (click the X in the upper right-hand corner of the window).

12. On the Restarting Windows window, you have a choice to reboot now or later. Select now **Yes** and then click **OK**.

---

*Public Key Infrastructure Up and Running*
Set up IP aliases

“Configuring IP aliases for the Web server” on page 24 contains a discussion of how Trust Authority configures ports on the Web server to process secure and non-secure transactions. If you want to use a different configuration, use IP aliases to define those ports.

Installing SecureWay Directory

Trust Authority uses the IBM SecureWay Directory to store and maintain information about certificates issued through the registration facility. Use the procedures in the following sections to install and set up the Directory software. You can install this software on a remote machine or on the same machine where you plan to install a Trust Authority server component.

Install Directory software

1. Insert the IBM SecureWay Directory Server CD in the CD-ROM drive and run the setup.exe program.
2. On the Choose the Language of the installation window, select the installation language and click Next.
3. On the Welcome window, click Next.
4. On the Select Components window, select Install the SecureWay Directory and Client SDK and click Next.
5. On the Choose Destination Location window, click Next to use the default installation path, or specify a different location and then click Next. If you receive a message about the installation partition not being an NTFS partition, click OK to continue.
6. On the Folder Selection window, click Next to accept the default program folder, or specify a different folder name and then click Next.
7. On the Configure window, clear all the boxes and click Next.
8. On the Start Copying Files for SecureWay Directory and Client SDK window, review the selections and click Next.
9. When prompted, click Yes to view the Readme file. After reviewing it, close the window (click the X in the upper right-hand corner of the window).
10. On the Setup Complete window, you have a choice to reboot now or later. Select now Yes and then click Finish.

Note: In a multiple machine configuration, each Trust Authority server must have the Directory client software installed before you run the Trust Authority configuration applet. To install this software, you must install the Directory Client option from the SecureWay Directory Server CD-ROM on each machine except the one where you just installed the Directory server software. The critical files that must be installed on each machine are ldap.dll and ldaploc1.dll.

Use the Directory with Trust Authority

Before you install or configure the Trust Authority server components, you need to understand how Trust Authority interacts with the Directory. To learn about Directory schema requirements and how to configure the Directory for Trust Authority, read “Using the SecureWay Directory With Trust Authority.” This document is available at the Trust Authority Web site.
Confirm system settings

Before installing Trust Authority, use the following procedure to ensure that the following services are in the states shown below.

1. Log in to Windows NT as the Trust Authority configuration user (typically cfguser).
2. Select **Start → Settings → Control Panel**.
3. Double-click **Services** and confirm the following states. The two highlighted service settings are critical:

<table>
<thead>
<tr>
<th>Service</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>Started</td>
</tr>
<tr>
<td>DB2 - DB2DAS00</td>
<td>Started</td>
</tr>
<tr>
<td>DB2 Governor</td>
<td>Manual</td>
</tr>
<tr>
<td>DB2 JDBC Applet Server</td>
<td>Manual</td>
</tr>
<tr>
<td>DB2 Security Server</td>
<td>Manual</td>
</tr>
<tr>
<td>IBM HTTP Server</td>
<td>Manual</td>
</tr>
<tr>
<td>WebSphere Servlet Service</td>
<td>Manual</td>
</tr>
</tbody>
</table>

4. Click **Close** and exit the Control Panel.

Installing Trust Authority

Use the following guidelines to install the Trust Authority product components.

- You must install all the server programs on the same platform, in this case Windows NT.
- If you previously installed IBM KeyWorks version 1.1.1, you must either install Trust Authority on a different machine, or remove the KeyWorks software and any associated applications before you start the Trust Authority installation program.
- If you are setting up Trust Authority in a multiple machine configuration, you must repeat the installation procedures until you have installed all server components on the intended machines.
- When you install the Client application or the RA Desktop applet, you first install an installation image. You must then distribute the image or make it available on your network so that users can run the installation program from a local Windows machine. For instructions on how to install, configure, and uninstall these programs, see the following documents:
  - *Trust Authority User’s Guide*
  - *Trust Authority RA Desktop Guide*
- If you did not restart the system after installing the prerequisite software, do so now. You must ensure that environment variables are correct before you install Trust Authority.
- Use PING or another network connectivity tool to verify that host names and IP addresses are valid and known to your network’s DNS server.

Install the server software

1. Log in to Windows NT by using the username and password that you identified for this purpose (typically cfguser). If necessary, see “Setting up Windows NT” on page 50 for assistance.
2. Shut down all active programs.
3. Place *IBM SecureWay Trust Authority for AIX and NT Disk 2* in a locally attached CD-ROM drive.
4. Select **Start → Run**, click **Browse** to change to the CD-ROM drive, and run setup.exe. For example:

```
drive:\WinNT\TrustAuthority\setup
```

If you are running the Setup program on a machine that has more than 256 MB of memory, you must add the `/z` switch to disable the memory check. For example:

```
drive:\WinNT\TrustAuthority\setup /z
```

5. On the Choose Setup Language window, select a language for this installation and click **OK**. The default value is **English**.

6. Review the information on the Welcome window, and click **Next**.

7. If you installed an independent version of IBM DB2 instead of the version provided with Trust Authority, the Choose Destination Location window appears. Click **Next** if you want to install the software in the default location (c:\Program Files\IBM\Trust Authority). Otherwise, click **Browse** to select or type a different destination folder, and then click **Next**.

8. On the Select Components window, use the following table as a guideline. Check the components you want to install, clear the components you do not want to install, and click **Next**.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Authority and Registration Authority server</td>
<td>Installs the main Trust Authority programs and the Registration Authority server software, including all files needed for the registration facility.</td>
</tr>
<tr>
<td>Certificate Authority and Audit server</td>
<td>Installs the Certificate Authority and Audit subsystem programs.</td>
</tr>
<tr>
<td>Directory server</td>
<td>Installs software that the Trust Authority components need to interact with the Directory.</td>
</tr>
<tr>
<td>Trust Authority Client</td>
<td>Installs an installation image for the Trust Authority Client application.</td>
</tr>
<tr>
<td>Registration Authority Desktop</td>
<td>Installs an installation image for the Trust Authority RA Desktop applet.</td>
</tr>
</tbody>
</table>

**Notes:**

- At this point, the Setup program determines whether the software required for the components you selected is installed and at the correct version level. If a prerequisite program is not available, the Setup program exits. Install the prerequisite software, and then start the installation procedure again.

- To prepare for database configuration, the Setup program also validates the username under which you logged in. If the username is longer than eight characters, the Setup program exits. Log in under a username that has eight or fewer characters, and then start the installation procedure again.

- If you select **Trust Authority and Registration Authority server**, and the Setup program detects that more than one version of IBM WebSphere Application Server or IBM HTTP Server is available, it prompts you to select the version you want to use.
9. On the Select Program Folder window, click Next if you want to create a program icon in the default program folder (Trust Authority). Otherwise, type or select the name of the folder you want to use, and then click Next.

10. On the Setup Complete window, click Finish to start the installation process. The system copies files to the requested locations and runs several programs to complete the installation of Trust Authority.

11. After the software is installed, restart the system.

**Change bootstrap values**

Use this procedure only if you want to change any of the default configuration values — values that you cannot change when running the configuration applet or after the system has been configured. You must make all bootstrap changes before you run the Trust Authority post-installation configuration program.

Trust Authority runs a bootstrap program as part of the post-installation process. Input to the bootstrap program is an SQL script named createconfig_start.sql that loads the configuration database with default values and creates database table definitions in the ConfigDataTbl database table. This table contains the system configuration data for all the Trust Authority components. Several values in this SQL script cannot be changed once the configuration process has started.

**Note:** Under critical circumstances where a default value may cause a problem in your operating environment, you can also change Trust Authority template files prior to configuration. For more information, contact your IBM support representative.

To change a bootstrap value, edit the createconfig_start.sql file. The default location for this file is c:\Program Files\IBM\Trust Authority\bin.

Use the following table as guidelines when making any changes:

- For Windows NT, you cannot change the DATABASE PATHNAME values.
- The distinguished names (DNs) for the Trust Authority RA, Directory administrator, and Audit subsystem are transparent to the user. If you want to change them, be sure to change only the common name (CN) attribute. The CA DN base you specify during configuration will be applied to the CN you select.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS_RO_KEYSIZE</td>
<td>Web server keyring key size. Options 0-3, as defined in the KeySize enumeration, are as follows:</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0 = 512</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 = 768</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 = 1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 = 2048</td>
<td></td>
</tr>
<tr>
<td>APP_DM</td>
<td>The DN of the Trust Authority RA. You can modify the CN only.</td>
<td>/C=US/O=Your Organization/OU=Trust Authority/CN=Trust Authority RA</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
<td>Default value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APP_CERT_LIFETIME</td>
<td>The lifetime of any non-CA certificate in the system (such as user, server, or RA certificates), specified in months. The value you specify must also be specified in the jonahca.ini.tpl and jonahra.ini.tpl files.</td>
<td>36</td>
</tr>
<tr>
<td>APP_LDAP_DIRADMIN_DN</td>
<td>The DN of the Directory administrator. You can modify the CN only.</td>
<td>/C=US/O=Your Organization/OU=Trust Authority/CN=DirAdmin</td>
</tr>
<tr>
<td>APP_COMM_PORT</td>
<td>The communication port that handles communications between the registration facility framework and the Trust Authority RA.</td>
<td>29783</td>
</tr>
<tr>
<td>APP_SEC_MECH</td>
<td>The application’s security mechanism. The default value disables the RA’s database encryption. Setting the value to 1 enables database encryption.</td>
<td>0</td>
</tr>
<tr>
<td>CA_IBM_CA_CERT_LIFETIME</td>
<td>The lifetime of the Trust Authority CA certificate, specified in months.</td>
<td>360</td>
</tr>
<tr>
<td>CA_IBM_ADMIN_PORT</td>
<td>The administrative port of the Trust Authority CA. The value you specify must also be specified on the PORT entry in the file, irgAutoCA.ini.tpl, which is located in the cfg directory.</td>
<td>1835</td>
</tr>
<tr>
<td>ADT_DN</td>
<td>The DN of the Audit subsystem. You can modify the CN only.</td>
<td>/C=US/O=Your Organization/OU=Trust Authority/CN=Trust Authority Audit</td>
</tr>
</tbody>
</table>

**Run the post-installation configuration program**

After you install the Trust Authority server software, you must run a post-installation configuration program, CfgPostInstall. You must run this program before you run the Setup Wizard to configure Trust Authority.

This program creates a Web server configuration file (httpd.conf) that allows the Web server to be started with parameters required by Trust Authority. It also prepares the Web server to run the configuration applet, creates the configuration database, and populates the database with default configuration data.

To run the post-installation configuration program:

1. Log in as the Trust Authority configuration user, cfguser.
2. Ensure that a temp directory exists on the server and that it is defined by the environment variable %TEMP%.
3. Select **Start → Programs → IBM SecureWay Trust Authority → Post Installation Configuration**.

4. Type `exit` to close the window.

CfgPostInstall prompts you to verify the cfguser account password, which was set when the account was created, and then prompts you to set and confirm the Control Program password. The password for cfguser controls access to the cfguser account and to the CfgApplet wizard page. The password for the Control Program restricts access to the Control Program. It is recommended that the password for the Control Program be different than the password for cfguser. The cfguser password you create must be a valid system password, not to exceed eight characters in length.

### Post-installation checklist

Use the following checklist to make sure that you are ready to begin configuring Trust Authority. For information about running the Setup Wizard, see the *Trust Authority Configuration Guide*.

1. Use your preferred Windows NT tools to back up the current system.

2. To aid in future problem resolution, create a backup copy of the Windows Registry to ensure that you have a list of all the installed software.

3. If you do not intend to use the default configuration values for the Web server ports, you must configure the IP aliases before you run the Setup Wizard. The configuration programs rely on these values when creating the CA certificate for your system. See "Configuring IP aliases for the Web server" on page 24 for a discussion of how Trust Authority configures and uses ports on the Web server for secure and non-secure transactions.

4. Decide on the distinguished names you want to use for the Trust Authority CA and its agents, the Directory administrator and the Directory root.

   If necessary, review the guidelines in "Using the SecureWay Directory With Trust Authority" to make sure that the DNs for these objects support your intended certification hierarchy. This document is available at the Trust Authority Web site.

5. Print the *Trust Authority Configuration Data Form* to become familiar with information you must have on hand before you configure the system. Use the form to record information about your system, such as your server host names and your preferred distinguished names.

   The configuration data form is available at the Trust Authority Web site.

6. To aid in configuration, take the following steps to set up a large, scrollable MS DOS environment on the machine where you plan to run the Setup Wizard. In a typical environment, the DOS window does not have a scroll bar and displays only 24 lines of information.

   a. Log in as the Trust Authority configuration user (typically cfguser).

   b. Select **Start → Settings → Control Panel**.

   c. Double-click the MS DOS Console.

   d. Select the **Layout** tab.

   e. In the **Screen Buffer Size** section, set **Height** to at least 1000 (you can specify any high number up to the maximum 9999) and click **OK**.
Run the backup utility

The Trust Authority backup utility, ta-backup, is a tool for saving configuration data that is not stored in any of the DB2 databases. The ancillary file data such as file permissions are also saved. Use DB2 utilities for backing up DB2 databases.

The backup utility accepts one parameter that identifies the directory where backup data is to be written. This backup directory is the root directory to be used for saving all data files. To avoid name conflicts within the backup directory, the backup utility saves files with the same directory structure as exists on the system being saved.

The following example illustrates the program syntax:

```plaintext
    ta-backup -d backup_directory
```

where:

- `-d backup_directory` is the directory to be used for data backup. The default path is `/usr/lpp/iau/backup`.

Follow these steps to run the ta-backup utility offline:

1. Log in as cfuser.
2. Optionally create the directory to which you want to back up Trust Authority configuration data. For example:
   ```plaintext
   mkdir "c:\Program Files\IBM\Trust Authority\my_tabackup"
   ```
3. Change to the Trust Authority bin directory. The default path is `c:\Program Files\IBM\Trust Authority\bin`.
4. Enter the following command, and specify the absolute path to where you want data to be backed up:
   ```plaintext
   ta-backup -d "c:\Program Files\IBM\Trust Authority\my_tabackup"
   ```

Upgrading the WebSphere Software

As part of the Trust Authority installation process, files are copied from the WebSphere Application Server for use by Trust Authority. If you upgrade the WebSphere software, or apply WebSphere software patches, the files copied by Trust Authority may no longer be valid. If any of the following files are replaced during an upgrade of the WebSphere product, you should copy them to the Trust Authority locations.

You need to make sure that the following directories are identical:

<table>
<thead>
<tr>
<th>WebSphere Directories</th>
<th>Trust Authority Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS_install_root\realms</td>
<td>TA_install_root\etc\realms</td>
</tr>
<tr>
<td>WAS_install_root\lib</td>
<td>TA_install_root\etc\lib</td>
</tr>
<tr>
<td>WAS_install_root\servlets</td>
<td>TA_install_root\etc\servlets</td>
</tr>
<tr>
<td></td>
<td>TA_install_root\pkrf\Domains\domain_name\etc\realms</td>
</tr>
<tr>
<td></td>
<td>TA_install_root\pkrf\Domains\domain_name\etc\lib</td>
</tr>
<tr>
<td></td>
<td>TA_install_root\pkrf\Domains\domain_name\etc\servlets</td>
</tr>
</tbody>
</table>

If you upgrade the WebSphere software, you must perform a deep copy (xcopy /s /e) of the updated WebSphere directories. For example, repeat and modify the following command for each WebSphere directory:
xcopy /s /e WAS_install_root\realms TA_install_root\etc\realms
After installing the Trust Authority server software, you must specify configuration values to control how the components are set up at your site. For example, you need to identify the locations of the server programs, specify distinguished names, and set up your registration domain.

During configuration, the system saves your values in an exportable file. This feature is useful for migration or for setting up multiple instances of Trust Authority that use the same platform and have similar configurations. When you install a new Trust Authority instance, you can import the saved values to use as a baseline for configuring the new system.

The Trust Authority product includes the Setup Wizard, an applet for specifying configuration options. Before you begin to configure your Trust Authority system, you need to understand the configuration process and decide how you want to set up the system in your environment. You need to have knowledge about your system on hand at the time you run the Setup Wizard. You also need to make sure that your system is properly configured before you attempt to use it.

The IBM SecureWay Trust Authority Configuration Guide documents how to prepare for configuration, specify configuration options, and prepare the system for use in a production environment. For example, it includes:

- Work sheets to help you gather information before you start the Setup Wizard.
- Guidelines for using the DN editor to specify a valid distinguished name.
- Recommendations for steps you should take before you release Trust Authority to your user community. Note that certain steps, such as changing the server passwords and backing up your newly configured system, are critical.
- Procedures for uninstalling the software.

Designed for use in a Web environment, the Configuration Guide provides:

- Task-oriented information, such as "How do I set up remote components?" or "How do I verify the configuration?"
- Conceptual information, such as "Tell me about registration domains" or "Tell me about the Directory".
- Reference information, such as detailed descriptions of the values you can specify when using the Setup Wizard.

You can access the Configuration Guide in any of the following ways:
After starting the Setup Wizard, click any **Help** button, then click the book icon while viewing online help.

Place the *Trust Authority Documentation* CD in a CD-ROM drive.

- Follow the path below to open the HTML version of the book (in English). For best performance, you may want to copy all files in the html directory to a local drive.
  \en_US\config\html\iauc.htm
- Follow the path below to open the PDF version of the book (in English). For best performance, you may want to copy this file to a local drive.
  \en_US\config\pdf\iaucmst.pdf
Getting started

After installing and configuring your Trust Authority system, you need to learn about administering it and using the graphical user interfaces it provides. The following sections direct you to documentation that can help you get started with Trust Authority. You should review these documents to learn how to do the following kinds of tasks:

- **Fine-tune system operations**, whether securing it for production or making ongoing performance adjustments
- **Run the RA Desktop** to administer issued certificates and requests for certificates
- **Obtain certificates**, whether using the browser enrollment forms provided with the registration facility or the Trust Authority Client application
- **Customizing registration processes**, such as modifying the front-end HTML forms for enrollment or including support for different certificate types

System administration

IBM SecureWay Trust Authority provides several tools to help you administer the system. For example, it includes:

- A utility for starting and stopping the server components in a secure, password-protected mode.
- A utility for setting secure passwords for the trusted component programs.
- A utility for authorizing administrative users to use the RA Desktop.
- A utility that enables the Trust Authority CA to cross-certify with another CA or to establish a CA hierarchy.
- A utility for checking the integrity of the audit database and archived audit records.
- A utility for archiving and signing the audit database.
- A configuration file editor that facilitates your ability to update configuration files. For example, you may want to fine-tune certain runtime controls for your processing environment.

The *IBM SecureWay Trust Authority System Administration Guide* documents these utilities and provides administrative guidelines. For example, it includes recommendations for administering the server components and their respective databases. It also documents the steps you must take to finalize the system’s setup and secure it for use in a production environment.
Designed for use in a Web environment, the *System Administration Guide* provides:

- Task-oriented information, such as "How do I stop the system?" or "How do I archive the audit database?"
- Conceptual information, such as "Tell me about cross-certification", "Tell me about the Trust Authority CA", or "Tell me about auditable events".
- Reference information, such as detailed descriptions of configuration file parameters.

To access the *System Administration Guide*, place the *Trust Authority Documentation* CD in a CD-ROM drive.

- Follow the path below to open the HTML version of the book (in English). For best performance, you may want to copy all files in the html directory to a local drive.
  \en_US\system\html\iaus.htm
- Follow the path below to open the PDF version of the book (in English). For best performance, you may want to copy this file to a local drive.
  \en_US\system\pdf\iausmst.pdf

**RA administration**

The RA server stores records about enrollment requests and issued certificates in an encrypted registration database. Evaluating enrollment requests and administering the database records are tasks that can be handled programmatically or by a human administrator.

Trust Authority provides an applet, the RA Desktop, that makes it easy for authorized registrars to process requests for certificates and take action on issued certificates.

The RA Desktop supports the following typical administrative tasks:

- Working with enrollment requests that are awaiting approval
- Changing the validity period for certificates that are about to expire
- Determining whether a certificate can be renewed
- Temporarily putting certificates on hold
- Permanently revoking certificates

The *IBM SecureWay Trust Authority Registration Authority Desktop Guide* documents the RA Desktop applet.

Designed for use in a Web environment, the *RA Desktop Guide* provides:

- Task-oriented information, such as "How do I install the RA Desktop", "How do retrieve a set of certificates that are about to expire?", or "How do I view a history of the actions taken on a certificate?"
- Conceptual information, such as "Tell me about registration domains" or "Tell me about the certificate life cycle".
- Reference information, such as detailed descriptions of the values a registrar can specify when using the RA Desktop.

You can access the *RA Desktop Guide* in the following ways:
After starting the RA Desktop, click any Help button, then click the book icon while viewing online help.

Place the Trust Authority Documentation CD in a CD-ROM drive.

- Follow the path below to open the HTML version of the book (in English). For best performance, you may want to copy all files in the html directory to a local drive.
  
  \en_US\desktop\html\iaud.htm

- Follow the path below to open the PDF version of the book (in English). For best performance, you may want to copy this file to a local drive.
  
  \en_US\desktop\pdf\iaudmst.pdf

## Registration and certification

IBM SecureWay Trust Authority provides two approaches for requesting and obtaining digital certificates:

- Using the browser enrollment forms that are provided with the registration facility, you can easily register for browser, server, and device certificates. When the request is approved, the certificate is downloaded automatically. You can also use the browser forms to preregister for certificates that can be used with a PKIX application. When the preregistration request is approved, information is provided that enables you to obtain the certificate at a convenient time.

- Using the Trust Authority Client application, you can easily load certificates for which you have been preregistered onto smart cards. You can then use the Client application to view information about a certificate, renew it, revoke it, or delete it. You can also import and export certificates between file storage systems and smart cards, or use the certificate to digitally sign files.

The IBM SecureWay Trust Authority User’s Guide documents the browser enrollment forms and the Trust Authority Client application.

Designed for use in a Web environment, the User’s Guide provides:

- Task-oriented information, such as “How do I install the Client application”, “How do I enroll for a browser certificate?”, or “How do I renew certificates that are about to expire?”

- Conceptual information, such as “Tell me about preregistration” or “Tell me about server certificates”.

- Reference information, such as detailed descriptions of the values a user can specify when using the Client application.

You can access the User’s Guide in the following ways:

- After starting the Client application, select Help → Help topics.

- After starting the Client application, click any Help button, then click the book icon while viewing online help.

- Place the Trust Authority Documentation CD in a CD-ROM drive.

  - Follow the path below to open the HTML version of the book (in English). For best performance, you may want to copy all files in the html directory to a local drive.
    
    \en_US\user\html\iauu.htm
Customization

IBM SecureWay Trust Authority provides flexibility for how you want to implement registration processes for your organization. For example, it allows you to control the following kinds of activities:

- The look and feel of the browser enrollment forms.
- Certification policies.
- The content of notification letters sent to users who register for certificates.
- Policy exits to handle different types of automated processing.

The *IBM SecureWay Trust Authority Customization Guide* documents the various ways that you can customize the registration facility.

Designed for use in a Web environment, the *Customization Guide* provides:

- Task-oriented information, such as "How do I add an enrollment field?" or "How do I change a certificate profile?"
- Conceptual information, such as "Tell me about preregistration.", "Tell me about business policy", or "Tell me about access controls".
- Reference information, such as detailed descriptions of certificate types and the registration facility configuration file.

To access the *Customization Guide*, place the *Trust Authority Documentation* CD in a CD-ROM drive.

- Follow the path below to open the HTML version of the book (in English). For best performance, you may want to copy all files in the html directory to a local drive.
  \en_US\custom\html\iaut.htm

- Follow the path below to open the PDF version of the book (in English). For best performance, you may want to copy this file to a local drive.
  \en_US\custom\pdf\iautmst.pdf
This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. 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 IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

**Trademarks and service marks**

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

IBM
AIX
AIX/6000
DB2
DB2 Universal Database
Netfinity
RISC System/6000
RS/6000
SecureWay
WebSphere
The Trust Authority program ("the Program") includes portions of the IBM WebSphere Application Server and the IBM HTTP Web Server ("IBM Servers"). You are not authorized to install or use the IBM Servers other than in connection with your licensed use of the Program. The IBM Servers must reside on the same machine as the Program, and you are not authorized to install or use the IBM Servers separate from the Program.

The Program includes portions of DB2 Universal Database. You are authorized to install and use these components only in association with your licensed use of the Program and IBM WebSphere Application Server for the storage and management of data used or generated by the Program and IBM WebSphere Application Server, and not for other data management purposes. For example, this license does not include inbound connections to the database from other applications for queries or report generation. You are authorized to install and use these components only with and on the same machine as the Program.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Pentium is a trademark of Intel Corporation in the United States, other countries, or both.

This program contains security software from RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. All rights reserved.

This program contains Standard Template Library (STL) software from Hewlett-Packard Company. Copyright (c) 1994.

- Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

This program contains Standard Template Library (STL) software from Silicon Graphics Computer Systems, Inc. Copyright (c) 1996–1999.

- Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

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

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


Numbers

4758 PCI Cryptographic Coprocessor
A programmable, tamper-responding cryptographic PCI-bus card offering high performance DES and RSA cryptographic processing. The cryptographic processes occur within a secure enclosure on the card. The card meets the stringent requirements of the FIPS PUB 140-1 level 4 standard. Software can run within the secure enclosure. For example, credit card transaction processing can use the SET™ standard.

A

Abstract Syntax Notation One (ASN.1)
An ITU notation that is 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 the use of a specific resource to authorized users.

ACL
Access control list.

action history
Accumulated events in the life cycle of a credential.

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

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

ASCII

ASN.1
Abstract Syntax Notation One.
asymmetric cryptography
Cryptography that uses different, asymmetric keys for encryption and decryption. Each user receives a pair of keys: a public key accessible to all, and a private key known only to the user. A secure transaction can occur when the public key and the corresponding private key match, 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 client
Any client in the system that sends audit events to the Trust Authority Audit server. Before an audit client sends an event to the Audit server, it establishes a connection with the Audit server. After the connection is established, the client uses the audit subsystem client library to deliver events to the Audit server.

audit log
In Trust Authority, a table in a database that stores one record per audit event.

Audit server
A Trust Authority server that receives audit events from audit clients and writes them to an audit log.

audit subsystem
In Trust Authority, a subsystem that provides the support for logging security-relevant actions. It conforms to recommendations in standard X9.57, of the standards set forth in Public Key Cryptography for the Financial Services Industry.

audit trail
Data, in the form of a logical path, that links a sequence of events. An audit trail enables tracing of transactions or the history of a given activity.

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

authorization
Permission to access a resource.

B

base64 encoding
A common means of conveying binary data with MIME.

Basic Encoding Rules (BER)
The rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract syntax.

BER
Basic Encoding Rules.

browser
See Web browser.

browser certificate
A digital certificate is also known as a client-side certificate. It is issued by a CA through an SSL-enabled Web server. Keys in an encrypted file enable the holder of the certificate to encrypt, decrypt, and sign data. Typically, the Web browser stores these keys. Some applications permit storage of the keys on smart cards or other media. See also digital certificate.

business process objects
A set of code used to accomplish a specific registration operation, such as checking the status of an enrollment request or verifying that a public key was sent.

business process template
A set of business process objects that are run in a specified order.
**bytecode**

Machine-independent code that is generated by the Java compiler and run by the Java interpreter.

**CA**

Certificate authority.

**CA certificate**

A certificate your Web browser accepts, at your request, from a CA it does not recognize. The browser can then use this certificate to authenticate communications with servers that hold certificates issued by that CA.

**CA hierarchy**

In Trust Authority, a trust structure whereby one CA is located at the top of the structure and up to four layers of subordinate CAs are located below. When users or servers are registered with a CA, they receive a certificate signed that is by that CA, and they inherit the certification hierarchy of the layers above.

**CA server**

The server for the Trust Authority Certificate Authority (CA) component.

**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.

**CDSA**

Common Data Security Architecture.

**certificate authority (CA)**

The software responsible for following an organization’s security policies and assigning secure electronic identities in the form of certificates. The CA processes requests from RAs to issue, renew, and revoke certificates. The CA interacts with the RA to publish certificates and CRLs in the Directory. See also digital certificate.

**certificate extension**

An optional feature of the X.509v3 certificate format that provides for the inclusion of additional fields in the certificate. There are standard extensions and user-defined extensions. Standard extensions exist for various purposes, including key and policy information, subject and issuer attributes, and certification path constraints.

**certificate policy**

A named set of rules that indicates the applicability of a certificate to a particular class of applications that have common security requirements. For example, a certificate policy might indicate whether a particular certification type allows a user to conduct transactions for goods within a given price range.

**certificate profile**

A set of characteristics that define the type of certificate wanted (such as SSL certificates or IPSec certificates). The profile aids in managing certificate specification and registration. The issuer can change the names of the profiles and specify characteristics of the desired certificate, such as the validity period, key usage, DN constraints, and so forth.

**certificate revocation list (CRL)**

A digitally signed, time-stamped list of certificates that the certificate authority has revoked. The certificates in this list should be considered unacceptable. See also digital certificate.

**certification**

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

**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 by another CA, both signatures are validated during validation of the certificate that the user presents.

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. Synonym for plaintext.

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.

code signing
A technique for signing executable programs with digital signatures. Code signing is designed to improve the reliability of software that is distributed over the Internet.

Common Cryptographic Architecture (CCA)
IBM software that enables a consistent approach to cryptography on major IBM computing platforms. It supports application software that is 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 Data Security Architecture (CDSA)
An initiative to define a comprehensive approach to security service and security management for computer-based security applications. It was designed by Intel, to make computer platforms more secure for applications.

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.

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

CRL
Certificate revocation list.

CRL publication interval
Set in the CA configuration file, the interval of time between periodic publications of the CRL to the Directory.

cross-certification
A trust model whereby one CA issues to another CA a certificate that contains the public key associated with its private signature key. A cross-certified certificate allows client systems or end entities in one administrative domain to communicate securely with client systems or end entities in another domain.

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.
daemon
A program that carries out tasks in the background. It is implicitly called when a condition occurs that requires its help. A user need not be aware of a daemon, because the system usually spawns it automatically. A daemon might live forever or the system might regenerate it at intervals. The term (pronounced *daemon*) 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. IBM developed it originally. DES has been extensively studied since its publication and is a well-known and widely used cryptographic system. DES is a symmetric cryptographic system. 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.

Data Storage Library (DL)
A module that provides access to persistent data stores of certificates, CRLs, keys, policies, and other security-related objects.

decrypt
To undo the encryption process.

DEK
Document encrypting key.

DER
Distinguished Encoding Rules.

DES
Data Encryption Standard.

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 that is 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. 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 has authority 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
*See* certification.

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 not valid). Thus, a digital signature cannot be copied from one message and applied to another because the summary, or hash, would not match. Any alterations to the signed message 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.

Directory
A hierarchical structure intended as a global repository for information related to communications (such as e-mail or cryptographic exchanges). The Directory stores specific items that are essential to the PKI structure, including public keys, certificates, and certificate revocation lists.

Data in the Directory is organized hierarchically in the form of a tree, with the root at the top of the tree. 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. Each entry consists of typed attributes. These provide information about the object that the entry represents.

Each entry in the Directory is bound with an associated distinguished name (DN). This is unique when the entry includes an attribute that is known to be unique to the real world object. Consider the following example DN. In it, the country (C) is US, the organization (O) is IBM, the organizational unit (OU) is Trust, and the common name (CN) is CA1.

\[ C=US/O=IBM/OU=Trust/CN=CA1 \]

Directory server
In Trust Authority, the IBM SecureWay Directory. This Directory supports LDAP standards and uses DB2 as its base.

Distinguished Encoding Rules (DER)
Provides constraints on the BER. DER selects just one type of encoding from those that the encoding rules allow, eliminating all of the sender’s options.

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

DL
Data Storage Library.

DN
Distinguished name.

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

domain
See security domain and registration domain.

DSA
Digital Signature Algorithm.

e-business
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
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.

end-entity
The subject of a certificate that is not a CA.

encrypt
To scramble information so that only someone who has the appropriate decryption code can obtain the original information through decryption.
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
In Trust Authority, the process of obtaining credentials for use over the Internet. Enrollment encompasses the requesting, renewing, and revoking of certificates.

enrollment attribute
An enrollment variable that is contained in an enrollment form. Its value reflects the information that is captured during the enrollment. The value of the enrollment attribute remains the same throughout the lifetime of the credential.

enrollment variable
See enrollment attribute.

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

F
File Transfer Protocol (FTP)
An Internet client/server protocol for use in transferring files between computers.

firewall
A gateway between networks that restricts the flow of information between networks. Typically, the purpose of a firewall is to protect internal networks from unauthorized use from the outside.

FTP
File Transfer Protocol.

G
gateway
A functional unit that allows incompatible networks or applications to communicate with each other.

H
HTML
Hypertext Markup Language.

HTTP
Hypertext Transaction Protocol.

HTTP server
A server that handles Web-based communications with browsers and other programs in a network.

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 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.
ICL
Issued certificate list.

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.

IniEditor
In Trust Authority, a tool used to edit configuration files.

instance
In DB2, an instance is a logical database management environment for storing data and running applications. It allows definition of a common set of configuration parameters for 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).

integrity checking
The checking of audit records that result from transactions with external components.

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 telecommunication networks and services. It is the leading publisher of telecommunication technology, regulatory, and standards information.

Internet
A worldwide collection of networks that provide electronic connection between computers. This enables them to communicate with each other via software devices such as electronic mail or Web browsers. 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 and uses similar technology. Technically, intranet is a mere extension of the Internet. HTML and HTTP are some of the commonalities.

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 over the Internet.

ISO
International Standards Organization.

issued certificate list (ICL)
A complete list of the certificates that have been issued and their current status. Certificates are indexed by serial number and state. This list is maintained by the CA and stored in the CA database.

ITU
International Telecommunication Union.
**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 that is written in the Java language. It 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 Virtual Machine (JVM)**
The part of the Java run-time environment responsible for interpreting bytecodes.

**K**

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

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

**KeyStore**
A DL for storing Trust Authority component credentials, such as keys and certificates, in an encrypted format.

**L**

**LDAP**

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

**M**

**MAC**
Message authentication code.

**MD2**
A 128-bit message-digest hash function, designed by Ron Rivest. It is used 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. It 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 authentication code (MAC)
A secret key that is shared between the sender and the recipient. The sender authenticates, and the recipient verifies. In Trust Authority, MAC keys are stored in the KeyStores for the CA and Auditing components.

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

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 cryptographic system, 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 depend 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

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.

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 that is 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.

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 identifier (OID)
An administratively assigned data value of the type defined in abstract syntax notation 1 (ASN.1).

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 that the ISO approved.

OSI
Open Systems Interconnect.

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.

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.

PKCS #11
See Public Key Cryptography Standards.

PKCS #12
See Public Key Cryptography Standards.

PKI
Public key infrastructure.

PKIX
An X.509v3-based PKI.

PKIX certificate management protocol (CMP)
A protocol that enables connections with PKIX-compliant applications. PKIX CMP uses TCP/IP as its primary transport mechanism, but an abstraction layer over sockets exists. This enables support for additional polling transports.

PKIX CMP
PKIX certificate management protocol.

PKIX listener
The public HTTP server that a particular registration domain uses to listen for requests from the Trust Authority Client application.

plaintext
Unencrypted data. Synonym for cleartext.

decrypt

policy exit
In a registration facility, an organization-defined program that is called by the registration application. The rules specified in a policy exit apply the organization’s business and security preferences to the enrollment process.
preregistration
In Trust Authority, a process that allows one user, typically an administrator, to enroll other users. If the request is approved, the RA provides information that allows the user to obtain the certificate at a later time using the Trust Authority Client application.

privacy
Protection from the unauthorized disclosure of data.

privacy-enhanced mail (PEM)
The Internet privacy-enhanced mail standard, that the Internet Architect Board (IAB) adopted 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. 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-on convention for inter-computer communication.

proxy server
An intermediary between the computer that is requesting access (computer A) and the computer that is being accessed (computer 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 by 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 specifies a standard syntax for certification requests.
- PKCS #11 defines a technology-independent programming interface for cryptographic devices such as smart cards.
- PKCS #12 specifies a portable format for storing or transporting a user’s private keys, certificates, miscellaneous secrets, and so forth.

public key infrastructure (PKI)
A standard for security software that is 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 must be 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).

RA
Registration authority.

RA Desktop
A Java applet that provides RAs with a graphical interface for processing requests for credentials and administering them throughout their lifetime.

RA server
The server for the Trust Authority Registration Authority component.

RC2
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 against exhaustive key search than DES 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.

registrar
A user who has been authorized to access the RA Desktop, to administer certificates and requests for certificates.

registration authority (RA)
The software that administers digital certificates to ensure that an organization’s business policies are applied from the initial receipt of an enrollment request through certificate revocation.

registration database
Contains information about certificate requests and issued certificates. The database stores enrollment data and all changes to the certificate data throughout its life cycle. The database can be updated by RA processes and policy exits, or by registrars.

registration domain
A set of resources, policies, and configuration options related to specific certificate registration processes. The domain name is a subset of the URL that is used to run the registration facility.

registration facility
A Trust Authority application framework that provides specialized means of enrolling entities (such as browsers, routers, e-mail, and secure client applications) and managing certificates throughout their life cycle.

registration process
In Trust Authority, the steps for validating 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, and can be automated or administered by human interaction.

repudiate
To reject as untrue; for example, to deny that you sent a specific message or submitted a specific request.
request ID
A 24- to 32-character ASCII value that uniquely identifies a certificate request to the RA. This value can be used on the certificate request transaction to retrieve the status of the request or the certificate that is associated with it.

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

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

Secure Electronic Transaction (SET)
An industry standard that facilitates secure credit card or debit card payment over untrusted networks. The standard incorporates authentication of cardholders, merchants, and card-issuing banks because it calls for the issuance of 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 requests for standard HTTP requests. SSL creates a session during which the exchange signals to set up communications between two modems need to occur only once. After that, communication is encrypted. Message integrity checking continues until the SSL session expires.

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

server
(1) In a network, a data station that provides functions 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 to enable a Web server to conduct SSL-based transactions. When a browser connects to the server by using the SSL protocol, the server sends the browser its public key. This enables authentication of the identity of the server. It also enables encrypted information to be sent to the server. See also CA certificate, digital certificate, and browser certificate.

servlet
A server-side program that gives Java-enabled servers additional functionality.

SET
Secure Electronic Transaction.

SGML
Standard Generalized Markup Language.

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

sign
To use your private key to generate a signature. The signature is a means of proving that you are responsible for and approve of the message you are signing.

signing/verifying
To sign is to use a private digital key to generate a signature. To verify is to use the corresponding public key to verify the signature.
Simple Mail Transfer Protocol (SMTP)
A protocol that transfers electronic mail over the Internet.

site certificate
Similar to a CA certificate, but valid only for a specific Web site. See also CA certificate.

smart card
A piece of hardware, typically the size of a credit card, for storing 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.

SSL
Secure Sockets Layer.

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

symmetric cryptography
Cryptography that uses the same key for both encryption and decryption. Its security rests in the key — revealing 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 cryptography.

symmetric key
A key that can be used for both encryption and decryption. See also symmetric cryptography.

target
A designated or selected data source.

TCP/IP

top CA
The CA at the top of a PKI CA hierarchy.

TP
Trust Policy.

transaction ID
An identifier provided by the RA in response to a preregistration enrollment request. It enables a user running the Trust Authority Client application to obtain the pre-approved certificate.

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 many ways exist to do this, the most secure form of multiple encryption is triple-DES with three distinct keys.

Trust Authority
An integrated IBM SecureWay security solution that supports the issuance, renewal, and revocation of digital certificates. These certificates can be used in a wide range of Internet applications, providing a means to authenticate users and ensure trusted communications.

trust domain
A set of entities whose certificates have been certified by the same CA.
trusted computer base (TCB)
The software and hardware elements that collectively enforce an organization’s computer security policy. Any element or part of an element that can effect security policy enforcement is security-relevant and part of the TCB. The TCB is an object that is bounded by the security perimeter. The mechanisms that carry out the security policy must be non-circumventable, and must prevent programs from gaining access to system privileges to which they are not authorized.

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. While 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

Unicode
A 16-bit character set that is defined by ISO 10646. The Unicode character encoding standard is an international character code for information processing. The Unicode standard encompasses the principal scripts of the world and provides the foundation for the internationalization and localization of software. All source code in the Java programming environment is written in Unicode.

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

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.

UTF-8
A transformation format. It enables information processing systems that handle only 8-bit character sets to convert 16-bit Unicode to an 8-bit equivalent and back again without loss of information.

V

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
Virtual Private Network.

W

Web browser
Client software that runs on a desktop PC and enables the user 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, and some can display only text. Most browsers can handle the major forms of Internet communication, such as FTP transactions.
Web server
A server program that responds to requests for information resources from browser programs. See also server.

WebSphere Application Server
An IBM product that helps users develop and manage high-performance Web sites. It eases the transition from simple Web publishing to advanced e-business Web applications. The WebSphere Application Server consists of a Java-based servlet engine that is independent of both the Web server and its underlying operating system.

World Wide Web (WWW)
That part of the Internet where a network of connections is established between computers that contain 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 putting into effect 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 certificates across secure Internet networks. The X.509 certificate defines data structures that accommodate procedures for distributing public keys that are 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 the certificate. It also allows the application to determine whether the certificate is on the CRL. X.509v3 CRLs can be constructed for a specific validity period. They can also be based on other circumstances that might invalidate a certificate. For example, if an employee leaves an organization, their certificate would be put on the CRL.
This bibliography lists the publications in the IBM SecureWay Trust Authority library. It also lists publications pertaining to related products that may assist you when installing, administering, or using a Trust Authority system.

**Trust Authority library**
- IBM SecureWay Trust Authority Up and Running
- IBM SecureWay Trust Authority Configuration Guide
- IBM SecureWay Trust Authority Registration Authority Desktop Guide
- IBM SecureWay Trust Authority User’s Guide
- IBM SecureWay Trust Authority System Administration Guide
- IBM SecureWay Trust Authority Customization Guide

**FirstSecure library**
- IBM SecureWay FirstSecure Planning and Integration
- Understanding the IBM SecureWay FirstSecure Framework
- IBM SecureWay Policy Director Up and Running
- IBM SecureWay Policy Director Administration Guide
- IBM SecureWay Policy Director Programming Guide and Reference
- IBM SecureWay Firewall for Windows NT User’s Guide
- IBM SecureWay Firewall for AIX User’s Guide
- IBM SecureWay Firewall for Windows NT Reference
- IBM SecureWay Firewall for AIX Reference
- IBM SecureWay Firewall for Windows NT Setup and Installation
- IBM SecureWay Firewall for AIX Setup and Installation
- IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
- IBM SecureWay Firewall VPN Client User’s Guide

**Related product library**
- IBM WebSphere Application Server Standard Edition Getting Started
- IBM DB2 Universal Database Quick Beginnings for UNIX
- IBM DB2 Universal Database Quick Beginnings for Windows NT
- IBM DB2 Universal Database Administration Guide
- IBM DB2 Universal Database Command Reference
- *IBM SecureWay Directory Administration Guide*
- *IBM SecureWay 4758 PCI Cryptographic Coprocessor Installation Manual*
- *IBM SecureWay 4758 Cryptographic Coprocessor CCA Support Program*
Index

Numerics
4758 coprocessor
  CA KeyStore 12
  CA support 6, 8
  encrypting CA key 26
  installing 27, 42
  integration with CA 26
  overview 8
  publications 91
  setting up 26
  storing CA key 27
  system requirements 17

A
access controls
  CA privileges 26
  Directory administrator privileges 26
  Directory privileges 25
  Directory root privileges 26
  RA Desktop privileges 5
  system 22
AIX
  access controls 22
  backing up 35
  backup utility 46
  bootstrap values 44, 57
  CD-ROM filesystem 34
  cfguser username 23, 45, 58
  disk partitions 33
  firewall considerations 22
  hardware configurations 18
  host name resolution 34
  installation guidelines 42
  installation roadmap 31
  installing 4758 coprocessor 42
  installing Directory server 37
  IP aliases 40
  operating system level 17
  post-installation checklist 46
  security considerations 21
  server platforms 17
  setting up 32
  software requirements 17
  system image 35
  system users 34
  verifying filesets 32
AIX/6000 operating system 17
architecture (continued)
  smart cards 11
Audit subsystem
  archiving 7
  database 7
  event masks 7
  installing on AIX 43
  installing on NT 55
  integrity checking 7
  KeyStore 12
  MACs 7
  overview 7

B
backup and recovery, key 10
backup images
  AIX 35, 46
  NT 51, 60
bootstrap values
  on AIX 44
  on NT 57
browser certificates 4

C
CD-ROM filesystem 34
CD-ROMs, product 29
CDSA 10
certificate authority (CA)
  4758 coprocessor 6, 8
  certificate revocation list 6
  cross-certification 6
  database 6
  DN entry 26
  hierarchy 6
  installing on AIX 43
  installing on NT 55
  integration with 4758 coprocessor 26
  issued certificate list 6
  KeyStore 12
  MACs 6
  overview 6
  protecting keys 26
  self-signed certificate 6
  serial number 6
  storing key in hardware 27
certificate extensions
  common 14
  customizing 14
certificate extensions (continued)
in Trust Authority 14
private 14
standard 14
certificate profiles
customizing 5
described 4
certificate revocation list (CRL) 6
certificate types 4
certificates
extensions 14
self-signed CA 6
trust hierarchy 6
X.509v3 support 13
cfgPostInstall program 45
cfguser username 23, 45, 50, 58
checklists
post-installation on AIX 46
post-installation on NT 59
Client application
documentation for 67
help for 67
installing 42, 55
overview 9
system requirements 20
client authentication 24
code signing 12
Common Data Security Architecture (CDSA) 10
common extensions 14
configuration
bootstrap values on NT 44, 57
data collection form 46, 59
Directory server 25
disk partitions in AIX 33
DOS environment setup 59
firewalls 22
overview of process 63
preparing for on AIX 46, 63
preparing for on NT 59, 63
server architecture 28
Web server 24
configuration data form 46, 59
Configuration Guide
accessing 63
overview 63
controlling server access 22
createconfig_start.sql file 44, 57
CRL 6
cross-certification 6
cryptographic algorithms 28
Customization Guide
accessing 68
overview 68
customizing
certificate extensions 14
certificate profiles 5
policy exits 5
registration domains 5
databases
audit data 7
CA data 6
Directory data 8
key backup and recovery 10
overview 8
registration data 4
reserved names 23
system requirements 17
datavg disk partition 33
DB2
advantages 8
audit database 7
CA database 6
data encryption 12
db2admin user 51
Directory database 8
installing 35
installing on AIX 35
installing on NT 51
publications 91
reserved names 23
system requirements 17
db2admin user 51
defining disk partitions in AIX 33
Directory administrator
DN entry 26
KeyStore 12
Directory schema 25
Directory server
access controls 25
CA DN 26
configuring 25
Directory administrator DN 26
installing on AIX 37, 43
installing on NT 54, 55
overview 8
publications 91
root DN 26
schema 25
software requirements 17
using with Trust Authority 37, 54
disk partitions
dbfsadtmp 34
dbfisibm 33
dbfsskrb 34
dbfsskRF 34
for AIX server 33
disk space
recommended for AIX 18
recommended for NT 18
sizing guidelines 18, 33
distinguished names (DN), defined 25
DN, defined 25
DNS 24, 25
documentation CD-ROM 14
domestic encryption edition 28
DOS environment 59

D
E encryption algorithms 28
enrollment
  browser forms 4
certificate types 4
  customizing 5
  notification letters 4
  overview 4
  policy exits 4
  preregistration 4, 9
  system requirements 20
exportability, cryptographic algorithms 28

F file systems
  CD-ROM 34
  for AIX server 33
  verifying 32
firewall security 22
FirstSecure
  integration with Policy Director 27
Planning and Integration 1, 27
publications 91
Redbook 1

G getting started
  with configuration 63
  with customization 68
  with enrollment 67
  with RA administration 66
  with system administration 65
  with Trust Authority 65
GSKIT
  upgrading on AIX 40

H hardware requirements
  4758 coprocessor on AIX 27, 42
  AIX 32
  confirm NT system 55
  database software on AIX 35
  database software on NT 51
  Directory server on AIX 37
  Directory server on NT 54
  HTTP Server on AIX 41
  HTTP Server on NT 52
  JDK on NT 52
  post-installation checklist, AIX 46
  post-installation checklist, NT 59
  server components on AIX 42
  server components on NT 55
  Web server on AIX 39
  Web server on NT 52
  WebSphere Server on AIX 39
  WebSphere Server on NT 53
  Windows NT 50
installp program 43
InstallShield program, server setup 55
integrity protection
  of audit records 7
  of CA records 6
international encryption edition 28
IP aliases
  described 24
  setting up on AIX 40
  setting up on NT 54
IPSec certificates 4
issued certificate list (ICL) 6

J Java
  upgrading on AIX 38

HTTPS protocol 24

I iauc.htm file 64
iaucmst.pdf file 64
iaud.htm file 67
iaudmst.pdf file 67
iaus.htm file 66
iausmst.pdf file 66
iautmst.pdf file 68
iau.htm file 67
iauumst.pdf file 68
IBM HTTP Server
  installing on AIX 39
  installing on NT 52
  upgrading on AIX 41
IBM Support Desk 15
ICL 6
installation
  4758 coprocessor on AIX 27, 42
  AIX 32
  confirm NT system 55
  database software on AIX 35
  database software on NT 51
  Directory server on AIX 37
  Directory server on NT 54
  HTTP Server on AIX 41
  HTTP Server on NT 52
  JDK on NT 52
  post-installation checklist, AIX 46
  post-installation checklist, NT 59
  server components on AIX 42
  server components on NT 55
  Web server on AIX 39
  Web server on NT 52
  WebSphere Server on AIX 39
  WebSphere Server on NT 53
  Windows NT 50
installp program 43
InstallShield program, server setup 55
integrity protection
  of audit records 7
  of CA records 6
international encryption edition 28
IP aliases
  described 24
  setting up on AIX 40
  setting up on NT 54
IPSec certificates 4
issued certificate list (ICL) 6

J Java
  upgrading on AIX 38
JDK
installing on NT 52
required level 17

K
key recovery 10
KeyStores 12

L
languages
  product differences 28
  supported 28
library, Trust Authority Web site 14, 15

M
machine types
  recommended for AIX 18
  recommended for NT 18
MACs
  for audit records 7
  for CA records 6
  in KeyStores 12
masking audit events 7
memory (RAM)
  recommended for AIX 18
  recommended for NT 18
message signing 12
migration
  backup utility on AIX 46
  backup utility on NT 60

N
national language support
  cryptographic algorithms 28
  encryption editions 28
  language differences 28
  overview 28
Netfinity servers 18
network security 21

O
object stores 11
operating systems
  for AIX servers 17
  for NT servers 17
operating systems (continued)
  for Setup Wizard 19

P
passwords
  for AIX servers 17
  for NT servers 17
  for Setup Wizard 19
physical security 21
PKCS #11 responses 9
PKCS #12 file, recovering 10
PKI, defined 10
PKIX, defined 10
PKIX CMP certificates 4, 9
Policy Director 27
policy exits
  customizing 5
  defined 4
post-installation configuration program 45, 58
preregistration
  browser enrollment 4
  file 9
  overview 9
  transaction ID 9
private extensions 14
processors
  recommended for AIX 18
  recommended for NT 18
product packaging 29
protocols
  for smart cards 11
  HTTP 24
  HTTPS 24
  LDAP 11
  PKIX CMP 10
  SSL 24
  supported in Trust Authority 12
public Web server 24
publications
  Configuration Guide 63
  Customization Guide 68
  described 14
  FirstSecure library 91
  RA Desktop Guide 66
  related product library 91
  System Administration Guide 65
  Trust Authority library 91
  User’s Guide 67

R
RA Desktop
  adding registrars 5
  documentation for 66
  help for 66
  installing 42, 55
ta-backup utility 46, 60
temp directory 50
transaction ID 9
Trust Authority configuration user 50
Trust Authority system
  4758 cryptographic support 8
  Audit subsystem 7
  Certificate Authority server 6
  Client application 9
  cryptographic standards 12
  database system 8
described 1
Directory server 8
features 1
installing on AIX 42
installing on NT 55
main server 3
Registration Authority server 3
system diagram 3
Web server 7
Trust Authority URLs 15
Trust Authority Web site 1, 15
trust hierarchy 6
trust model
code signing 12
data encryption 12
KeyStores 12
message signing 12
Unicode support 28
upgrading WebSphere 60
URLs
  FirstSecure Framework Redbook 1
  HTTP server publications 25
  Readme file 14
  Trust Authority home page 1, 14, 15
  Trust Authority library page 14, 15
  Trust Authority support page 15
User’s Guide
  accessing 67
  overview 67
UTF-8 encoding 28

Version 3 Release 7.0

Windows NT
  access controls 22
  backup utility 60
cfguser username 23, 50
  firewall considerations 22
hardware configurations 18
installation guidelines 55
installation roadmap 49
installing Directory server 54
IP aliases 54
operating system level 17
post-installation checklist 59
required settings 55
security considerations 21
server platforms 17
setting up 50
software requirements 17

X.509v3 certificates 13

VPN certificates 4