Tivoli® SecureWay® Public Key Infrastructure

User’s Guide

Version 3  Release 70

SH09-4531-02
Contents

Chapter 1. About Trust Authority ........................................................................... 1

Chapter 2. Overview ................................................................................................. 3

Chapter 3. How do I...? ......................................................................................... 5

  Access the enrollment Web page ................................................................. 5
  Enroll using a browser ...................................................................................... 5
    Request a browser certificate ......................................................................... 6
    Enroll a server or device ............................................................................... 7
    Preregister someone .................................................................................... 8
    Check on enrollment status ......................................................................... 10
  Use a browser to manage certificates .......................................................... 10
    Suspend a certificate ................................................................................... 11
    Renew a certificate ...................................................................................... 11
    Revoke a certificate .................................................................................... 12
    Cancel active requests .............................................................................. 13
    Work with multiple certificates .................................................................. 13
    Issue a key backup request ....................................................................... 13
    Issue a key recovery request ..................................................................... 13
  Install the Client application ....................................................................... 14
  Enable a Physical Smart Card ..................................................................... 15
  Access the Client application ..................................................................... 16
  Enroll using the Client .................................................................................. 17
    Use a preregistration file to enroll ............................................................ 17
    Use a transaction ID to enroll .................................................................... 17
  Use the Client to manage certificates .......................................................... 18
    Delete a certificate or a pending request .................................................. 18
    Export a certificate from a smart card to a file ....................................... 18
    Import a certificate from a file to a smart card ....................................... 18
    Move a certificate to a different smart card .......................................... 19
    Open a certificate to view details .............................................................. 19
    Suspend a certificate ................................................................................ 19
    Renew a certificate ................................................................................... 19
    Renew expiring certificates ..................................................................... 20
    Revoke a certificate .................................................................................. 20
    Sign a file ................................................................................................. 21
  Work with a list of certificates ..................................................................... 21
About 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 ensure confidentiality.

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

- A trusted Certificate Authority (CA) manages the complete 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 ensures 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.
Overview

When an organization has secure applications protected by Trust Authority, only users with the proper credentials can access those applications. Someone who wants a credential, such as a digital certificate, can request it by providing appropriate information. Data in the enrollment request is the basis for the decision to approve the request or reject it. If an enrollment request is approved, the Trust Authority Registration Authority (RA) processes the request, and the Trust Authority Certificate Authority (CA) issues the certificate. Records of enrollment requests and certificates are stored in an encrypted registration database.

A Trust Authority system offers more than one way to request a certificate:

- The Trust Authority enrollment forms, available on a Web page.
- The Trust Authority Client application, which runs under Microsoft Windows.

Your organization can use either method of enrollment or both methods, whatever best suits its enrollees and its business policies.

The enrollment forms enable you to submit the necessary information to request a certificate and then return to get the response from the Trust Authority registration facility. You can apply for a browser certificate, a server certificate, or a device certificate. You can also preregister for a certificate to access a PKIX-compliant application. You can also return to the enrollment Web page to manage the certificates you receive directly from enrolling there.

The Client application offers a simpler process, designed for users who have already been preregistered. The application also provides dialogs and commands to help you to obtain and then manage your certificates.

This guide supports you in any of these enrollment tasks.
How do I...?

The topics in this section provide:

- Instructions for each phase of enrolling for a certificate on the Trust Authority enrollment Web page, and for using that page to manage browser certificates you obtained there.
- Instructions for using the Trust Authority Client application to request a certificate after preregistration, or to manage and use your certificates.

Access the enrollment Web page

To access the Web page for enrollment:

1. Make sure your workstation meets the requirements listed in "System requirements for browser enrollment" on page 37.
2. Get your organization’s URL for accessing the enrollment Web page. The URL will have the following format:
   http://MyPublicWebServer/MyDomain/index.jsp
3. Open your browser and enter the URL:
   - In Netscape, type the URL in the text box at Location.
   - In Internet Explorer, type it in the text box at Address.
4. Press the Enter key.
   The Trust Authority enrollment Web page is displayed. For a default installation, the name of the page is Credential Central.
5. If you are using the Trust Authority enrollment services for the first time, click install our server’s CA certificate.
   This certificate enables your browser to authenticate communications from the enrollment services. The next time you use these services, you can omit this step.

Enroll using a browser

The topics in this section describe how to use your Web browser to request a certificate on the Trust Authority enrollment page.

If you are using the enrollment services for the first time, you must obtain a CA certificate for your Web browser before proceeding. After that, you can use the enrollment pages repeatedly.
Depending on how the registration facility was customized for your organization, the procedures for getting a valid certificate may vary. The following topics provide basic steps. Contact your system administrator for procedures appropriate for your site.

**Request a browser certificate**

To obtain a browser certificate through your Web browser:

1. **Access** the enrollment Web page from your browser.
2. At **Enrollment Type**, open the list and select **Browser certificate**.
3. At **Action**, select **Enroll**.
4. Click **OK**.

The enrollment form you requested is displayed.

Follow the instructions on the Web page to complete the fields on the form. “Web page enrollment form” on page 33 describes the fields. The form has the following sections:

- **A Registration Information** section with text boxes where you supply information about yourself.
- **A Certificate Request Information** section with text boxes where you supply information about the certificate you want. If you do not supply values in the section’s optional fields, Trust Authority supplies defaults that are associated with the type of certificate you are requesting.

Pay particular attention to the following fields:

**Type of Certificate**
Select the **kind of browser certificate** that your organization wants you to present to have. “Supplied certificate types” on page 35 describes the certificate types.

**Install CA certificate to Browser**
Click to get a corresponding **CA certificate** that is compatible for the certificate type. If you click this button, the CA certificate is downloaded immediately.

This certificate enables your browser to authenticate communications from Trust Authority. If for some reason you already have the same CA certificate, you do not need another one.

**E-mail Address**
To select **E-mail Notification**, you must supply your e-mail address.

**E-mail Notification**
Select this to receive e-mail about the outcome of your request.

**Challenge Response**
Be sure to remember the case-sensitive **Challenge Response** you supply. You will need to know it later to check the status of the enrollment request.

**Common Name**
The **Common Name** field is pre-filled with information that you specify for **First Name** and **Last Name**. If you later go back to modify your first or last name entries, the change may not be reflected automatically in your common name. If not, be sure to update the **Common Name** field with your revised **First Name** and **Last Name** values before submitting the registration form.

**Domain Name**
Supply the host name of the machine where the certificate is being installed, if it
is related to the use of the certificate. This field is optional for browser
certificates; use it only if you have been instructed to do so.

6. Click **Submit Enrollment Request**.
   After Trust Authority receives the enrollment form, the following occurs:
   - If the form contains errors, it shows you the errors. Make the changes and click **Resubmit Enrollment Request**.
   - If the form contains no errors, another Web page displays your request ID.

7. Make sure to record your request ID. It identifies you later so that you can check on the status of the request and receive your certificate when it is ready. Do one of the following, as described on the Web page:
   - Bookmark the Web page so that you can return easily to this display and check on your certificate.
   - Record the request ID so that you can supply it when you return.
   - Wait for the request ID to come by e-mail.

**Enroll a server or device**

Any server or device you enroll for must have specific characteristics as defined in this guide. “Server or device certificates” on page 29 describes these characteristics.

To obtain a server or device certificate through your Web browser:

1. **Access** the enrollment Web page from your browser.
2. At **Enrollment Type**, open the list and select **Server or Device certificate**.
3. At **Action**, select **Enroll**.
4. Click **OK**.
   The enrollment form you requested is displayed.
5. Follow the instructions on the Web page to complete the fields on the form. “Web page enrollment form” on page 33 describes the fields. The form has the following sections:
   - A **Registration Information** section with text boxes where you supply information about yourself.
   - A **Certificate Request Information** section with text boxes where you supply information about the certificate you want for the server or device. If you do not supply values in the section’s optional fields, Trust Authority supplies defaults that are associated with the type of certificate you are requesting.

Pay particular attention to the following fields:

**Type of Certificate**
Select the kind of server or device certificate that your organization wants you to request. “Supplied certificate types” on page 35 describes the certificate types.

**Save CA certificate to File**
Click to get a corresponding CA certificate that is compatible for the certificate type. Your browser will prompt you for a path. If you click this button, the CA certificate is downloaded immediately.
This certificate enables the server or device to authenticate communications from Trust Authority. If for some reason you already have the same CA certificate, you do not need another one.

E-mail Address
To select E-mail Notification, you must supply your e-mail address.

E-mail Notification
Select this to receive e-mail about the outcome of your request.

Challenge Response
Be sure to remember the case-sensitive Challenge Response you supply. You will need to know it later to check the status of the enrollment request.

Common Name
The Common Name field is pre-filled with information that you specify for First Name and Last Name. If you later go back to modify your first or last name entries, the change may not be reflected automatically in your common name. If not, be sure to update the Common Name field with your revised First Name and Last Name values before submitting the registration form.

Domain Name
Supply the host name of the machine where the certificate is being installed, if it is related to the use of the certificate. This field is optional for server certificates; if you include it, identify the machine where the Web server is installed. The Domain Name is required for IPSec certificates; you must identify the IPSec device where the certificate will be installed.

6. Click Submit Enrollment Request.

After Trust Authority receives the enrollment form, the following occurs:

- If the form contains errors, it shows you the errors. Make the changes and click Resubmit Enrollment Request.
- If the form contains no errors, another Web page displays your request ID.

7. Make sure to record your request ID. It identifies you later so that you can check on the status of the request and receive your certificate when it is ready. Do one of the following, as described on the Web page:

- Bookmark the Web page so that you can return easily to this display and check on your certificate.
- Record the request ID so that you can supply it when you return.
- Wait for the request ID to come by e-mail.

Preregister someone
You can use the enrollment services to preregister yourself or someone else for a certificate to access a PKIX-compliant application. Later they can download the certificate while they are using the Trust Authority Client application.

To preregister someone through your Web browser:

1. Access the enrollment Web page from your browser.
2. At Enrollment Type, open the list and select Certificate preregistration.
3. At Action, select Enroll.
4. Click **OK**.
   The enrollment form you requested is displayed.

5. Follow the instructions on the Web page to complete the **fields** on the form. "Web page enrollment form" on page 33 describes the fields. The form has the following sections:
   - A **Registration Information** section with text boxes where you supply information about the person you are preregistering. You also supply here some information that will enable you to check on the status of your request.
   - A **Certificate Request Information** section with text boxes where you supply information about the certificate you want. If you do not supply values in the section’s optional fields, Trust Authority supplies defaults that are associated with the type of certificate you are requesting.

Pay particular attention to the following fields:

**Type of Certificate**
Select the type of certificate that is needed by the person you are preregistering. “Supplied certificate types” on page 35 describes the certificate types.

**E-mail Address**
To select **E-mail Notification**, you must supply your own e-mail address.

**E-mail Notification**
Select this to receive e-mail about the outcome of your request.

**Challenge Response**
Be sure to remember the case-sensitive **Challenge Response** you supply. You will need to know it later to check the status of the enrollment request.

**Common Name**
The **Common Name** field is pre-filled with information that you specify for **First Name** and **Last Name**. If you later go back to modify your first or last name entries, the change may not be reflected automatically in your common name. If not, be sure to update the **Common Name** field with your revised **First Name** and **Last Name** values before submitting the registration form.

**Domain Name**
Supply the host name of the machine where the certificate is being installed, if it is related to the use of the certificate. This field is optional for preregistration certificates; use it only if you have been instructed to do so.

6. Click **Submit Enrollment Request**.
   After Trust Authority receives the enrollment form, the following occurs:
   - If the form contains errors, it shows you the errors. Make the changes and click **Resubmit Enrollment Request**.
   - If the form contains no errors, another Web page displays your request ID.

7. Make sure to record your request ID. It identifies you later so that you can check on the status of the request and receive your certificate when it is ready. Do one of the following, as described on the Web page:
   - Bookmark the Web page so that you can return easily to this display and check on your certificate.
   - Record the request ID so that you can supply it when you return.
Check on enrollment status

To check the status of your enrollment request, either return to the Web page you bookmarked during enrollment, or complete the following steps:

1. Access the enrollment Web page.
2. At Type of Enrollment, select the type of enrollment you requested.
3. At Action, select Check Status.
4. Click OK.
   The display contains fields where you must authenticate your identity before you can get any information about your request.
5. Supply information in the fields:
   - At Request ID, type the request ID you were shown after you submitted the enrollment form.
   - At Challenge Response, type the same Challenge Response you supplied on the enrollment form.
6. Click Check Enrollment Status.
   A message indicates the current status of your request.
   - If your request is still pending, you can return later and check again.
   - If your request was approved, the type of request determines what happens next:
     **Browser certificate**
     The browser certificate is downloaded immediately to your browser.
     **Server or device certificate**
     Your browser prompts you to select a format and specify a path, and then the server or device certificate is downloaded to that path.
     **Certificate preregistration**
     The certificate is not delivered until the person you preregistered requests it from the Trust Authority Client application.
     Instead, you see information that the prospective certificate holder needs to request the certificate: a transaction ID, a password, and the URL of the RA that approved the request.

     **Note:** If desired, you can give them a preregistration file. This can be used, along with the password, when requesting the certificate. To get a copy of the file, click Save Preregistration File and specify a path for the file.

Use a browser to manage certificates

On the enrollment Web page, you can also renew or revoke a browser certificate you received. If necessary, you can put it on hold instead of revoking it permanently. This does not apply to certificates for which you preregistered.

**Note:** If you receive an error while using Microsoft Internet Explorer to renew or revoke certificates, it may be because you are unable to establish a client-authenticated SSL connection.
session with the Web server. To resolve this problem, select **Tools → Internet Options** in the browser. On the Internet Options Settings window, select the **Advanced** tab and click on the **Restore Defaults** button. This will reactivate SSL version 3.0. Click **OK** and close the browser. Restart Internet Explorer and try to connect to the server again.

### Suspend a certificate

You can suspend a browser certificate that you obtained directly from the enrollment Web page.

**Note:** If you received your certificate while using the Client application, you must use that application to suspend the certificate.

To suspend your certificate:

1. **Access** the enrollment Web page.
2. At **Type of Enrollment**, select **Browser Certificate**.
3. At **Action**, select **Suspend**.
4. Click **OK**.
   
The display contains information that identifies you and the certificate.
5. Examine the information to make sure that this is the certificate you want to suspend.
6. Click **Suspend Certificate**.

*Note:* If you want to reactivate a suspended certificate, you must contact the RA Administrator before the certificate’s grace period expires. Once the grace period expires, a suspended certificate cannot be reactivated.

### Renew a certificate

You can renew a browser certificate that you obtained directly from the enrollment Web page.

**Note:** If you received your certificate while using the Client application, you must use that application to renew the certificate.

To renew your certificate:

1. **Access** the enrollment Web page.
2. At **Type of Enrollment**, select **Browser Certificate**.
3. At **Action**, select **Renew**.
4. Click **OK**.
   
   A renewal form is displayed.
5. Examine the form to verify that this is the certificate that you want to renew.
6. Change values of the editable fields, if desired. *Web page enrollment form* on page 33 describes the fields.

**E-mail Address**

To select **E-mail Notification**, you must supply your e-mail address.
E-mail Notification
Select this to be notified by e-mail of the outcome of your request.

Challenge Question
You can change the question you will be asked when you check on your request.

Challenge Response
Be sure to remember the case-sensitive Challenge Response you supply. You will need to know it later to check the status of the enrollment request.

For Internet Explorer
- Follow instructions on the form if you want to change the provider for your cryptographic service.
- Decide whether to generate a new key set or reuse the existing one. For a new key set, you have the option of naming it yourself.
- Select Additional Security Options to request further security measures from Microsoft Internet Explorer, if desired.

7. Click Renew Certificate.
8. Retain your Request ID when it is displayed, so that you can check on the status of your request later. “Check on enrollment status” on page 10 describes how to check the status of your request.

Revoke a certificate
You can revoke a browser certificate that you obtained directly from the enrollment Web page.

Note: If you received your certificate while using the Client application, you must use that application to revoke the certificate.

To revoke your certificate:
1. Access the enrollment Web page.
2. At Type of Enrollment, select Browser Certificate.
3. At Action, select Revoke.
4. Click OK.
   Information identifying the certificate is displayed.
5. Examine the information to verify that this is the certificate you want to revoke.
6. At Reason, select a reason for revoking the certificate. “Reasons for revoking a certificate” on page 36 describes the valid reasons.
7. At Date the certificate is no longer valid, specify when to revoke the certificate. Select either the current date or a date in the past. If the reason is associated with a date, use that date. For example, if you suspect that your key was compromised, select the date you think that happened.
8. Click Revoke Certificate.
Cancel active requests

If you submit a request to renew a certificate, revoke a certificate, or suspend a certificate, and then attempt to cancel the request, the browser returns an error such as "Document contains no data". It will also be unable to redisplay the enrollment Web page.

This problem can occur if the browser transmits the request to the RA server before prompting you to present a certificate for authentication. When the certificate does not accompany the request, an error is returned. This is normal browser behavior. In this situation, the browser has no knowledge of which request needs to be canceled after you click the Cancel button.

Work with multiple certificates

If you submit a request to renew a certificate, revoke a certificate, or suspend a certificate, and then return to the enrollment Web page to work with another certificate, you will be unable to do so until you exit the browser and restart it. This is normal browser behavior. You must clear the current certificate from the browser cache before attempting to manage another one.

Likewise, after you download a certificate, you cannot renew it or revoke it in the same browser session. You must exit the browser before attempting to manage a newly installed certificate.

Issue a key backup request

You can request that a backup be created for a certificate and its private key. The PKCS #12 file you use as input to this request gets created when you export a certificate from a supported browser or the Client application. The PKCS #12 file can later be retrieved by issuing a key recovery request.

To issue a key backup request:

1. Get your organization’s URL for accessing the Key Backup Request Web page. The URL will have the following format:
   http://MyPublicWebServer/MyDomain/KeyBackup_Request.jsp
2. Open your browser and enter the URL:
   - In Netscape, type the URL in the text box at Location.
   - In Internet Explorer, type it in the text box at Address.
3. Press the Enter key.
   - The Trust Authority Key Backup Request Web page is displayed.
4. At PKCS #12 File, type the path and file name or click Browse to specify the exported PKCS #12 file that contains the certificate to be backed up.
5. At PKCS #12 File Password, type the password specified when this file was created.
6. Click Submit Key Backup Request.
   - A message displays indicating the status of this request.

Issue a key recovery request

You can issue a request to retrieve a certificate and its private key from a backup previously created by a key backup request. Upon approval of the recovery request by the RA Administrator, the PKCS #12 file is available and ready for you to download it. The password for the file is not provided since it should be known to you already. The RA
Administrator can, however, display the attributes of the file, including password, should the requester need that information. The mechanism for delivery of that information is typically defined by the enterprise (for example, electronic mail or some other means of correspondence).

After submitting the key recovery request, you can check the status to determine if the request is approved, rejected, or pending.

To issue a key recovery request:

1. Get your organization’s URL for accessing the Key Recovery Request Web page. The URL will have the following format:
   
   http://MyPublicWebServer/MyDomain/KeyRecovery_Request.jsp

2. Open your browser and enter the URL:
   - In Netscape, type the URL in the text box at Location.
   - In Internet Explorer, type it in the text box at Address.

3. Press the Enter key.
   
   The Trust Authority Key Recovery Request Web page is displayed.

4. At Type of Certificate, select the type of certificate you want to recover from the drop-down list.

5. At First Name, type your first name.

6. At Last Name, type your last name, family name, or surname.

7. At Common Name, type a name to identify the certificate request associated with the PKCS #12 file. Typically, this is the person’s full name.

8. Click Submit Key Recovery Request.
   
   The request goes to the RA Administrator for approval and the Check Key Recovery Status page is displayed.

9. Click Check Key Recovery Status to determine the status of your request.
   
   When the RA Administrator approves the request, the Key Recovery Request – Status Completed page is displayed.

10. Click Save Recovered PKCS #12 File to download and save the recovered file.

### Install the Client application

Installing the Trust Authority Client is a two-part process. When installing the server software, a system administrator must select Trust Authority Client to install the installation image for the application. The administrator must then distribute the image or make it available on your network so that you can run the installation program from your workstation.

Use the following procedure to run the Client application installation program, TACInst.exe.

1. Make sure your workstation meets the requirements listed in “System requirements for the Client application” on page 37.

2. Follow your organization’s instructions to copy, access, or download the Client installation image.
3. Shut down all active programs.

4. Select Start → Run, click Browse to locate the TACInst.exe file, and click OK to run the program.

5. Review the instructions on the Welcome window, and click Next.

6. On the Choose Destination Location window, 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.

   **Note:** If you previously installed a Trust Authority component on this workstation, the software will be installed automatically in a TAClient subdirectory at the same location. You will not be prompted for a destination location.

7. On the Select Program Folder window, click Next if you want to use the default program folder (IBM SecureWay Trust Authority). Otherwise, type or select the name of the folder you want to use and then click Next.

8. On the Open Smart Card window, type a password for your virtual smart card, type the same password again to confirm it, and click Next. You must specify this same password, which cannot have more than eight characters, when you start the Client application.

   At this point, the system copies files to the requested installation location, and runs programs to complete the installation of the Client application.

9. On the Setup Complete window, indicate whether you want to restart Windows now or later and then click Finish. If you choose to restart the system later, you must do so before attempting to use the Client application.

   After the installation is complete, Trust Authority Client is in your Start menu under Programs → IBM SecureWay Trust Authority.

**Usage Notes:**

- If you receive an error about not being able to find CSSM32.dll in the path, run the Client application installation program again. This should clear the error.

- If the Sun Java Runtime Environment (JRE) or Java Development Kit (JDK) was previously installed on the machine where you are installing the Client, and you receive an error about the JRE not being found, update the machine’s PATH variable to ensure that it includes the installed location of the jre.exe program.

**Enable a Physical Smart Card**

You must take the following steps after you install the Trust Authority Client application to be able to access and store certificates on a physical smart card.

1. Follow the procedures that came with your smart card to install the card and software. For example, you might want to install one of the following products:

   - IBM Smart Card Security Kit for Desktop Systems (for the serial version)
   - IBM Smart Card Security Kit for Notebook Computers (for the PCMCIA version)

2. Edit the TAClient.ini file. The default path for this file is c:\Program Files\IBM\Trust Authority\TAClient.

3. Change the [KeyStore] section as follows:
4. Change the [SmartCard] section as follows:

   Change:
   [SmartCard]
   Model=PKCS11_STORAGE_MODEL
   Guid=EABA7C01-13BC-11d3-B150-002035C00173
   LibraryName=
   to:
   [SmartCard]
   Model=PKCS11_STORAGE_MODEL
   Guid=EABA7C01-13BC-11d3-B150-002035C00173
   LibraryName=c:\winnt\system32\W32pk2ig.dll

   Note: LibraryName in this example shows the default location of W32pk2ig.dll for a
   Windows NT system installed on the C: drive; the location of this file on your
   system may be different.

5. Enter the following commands to run the initsc program. You will not be prompted for
   passwords (the passwords remain as you set them when installing the physical smart
   card).

   cd "c:\Program Files\IBM\Trust Authority\bin"
   initsc -e ee -i c:\Program Files\IBM\Trust Authority\TAClient\TAClient.ini

When using the smart card with the Client application, be aware that the card can hold a
512–bit key pair, a 1024–bit key pair, and their corresponding certificates. If you try to
generate a second 512–bit key pair or a second 1024–bit key pair, you will receive an out of
memory error message.

Access the Client application

Use the Client application to request and then store a certificate on your virtual or physical
smart card after someone has preregistered you. You can also use the Client application to
manage the certificates on your smart cards, and to manage the smart cards themselves. All
these certificates are for accessing PKIX-compliant applications.

To access the Client application:

1. If you want to use your physical smart card, insert it.

2. On your Windows taskbar, select Start → Programs → IBM SecureWay Trust Authority
   → Trust Authority Client.

3. On the splash screen, click OK.
   The Open Smart Card dialog is displayed. It contains a list of your smart cards that are
defined to the Client application. Page 13 describes the dialog.

4. At Smart Card, select the smart card you want to open.

5. At Password, type your smart card password.

6. Click OK.
   The Smart Card View window is displayed. Page 38 describes the window.
Note: If you have certificates that are due to expire soon, the Client application displays these so you can decide whether to renew any of them. “Renew expiring certificates” on page 26 describes what to do if this happens.

Enroll using the Client

Before you can use the Client application to request a certificate, you must preregister on the Trust Authority enrollment Web page. Your registrar, a user authorized to administer registration requests, will probably preregister you.

After you receive the preregistration information, use the Client application to request a certificate. The kind of preregistration information you receive determines the Client menu option to select:

- A preregistration file
- A transaction ID

Use a preregistration file to enroll

In the Smart Card View window:

1. Open the Certificate menu and click New → Using a Preregistration File.
   The New Certificate Using a Preregistration File dialog is displayed. Page 41 describes the dialog.
2. Complete the fields on the dialog and click Next.
   What you see next on the dialog varies at the option of your organization. You might see:
   - Attributes and their values, that describe your certificate request.
   - Fields near the bottom of the display, where you can change some attribute values by typing over them.
3. Make the necessary changes, if any.
4. Click Next to submit your request.
5. In the confirmation box, click Finish.

After the Registration Authority approves your request, your certificate is automatically stored on the smart card you have open.

Use a transaction ID to enroll

In the Smart Card View window:

1. Open the Certificate menu and click New → Using a Transaction ID.
   The New Certificate Using a Transaction ID dialog is displayed. Page 41 describes the dialog.
2. Complete the fields.
3. Click Next to submit your request.
4. In the confirmation box, click Finish.

After the Registration Authority approves your request, your certificate is automatically stored on the smart card you have open.
Use the Client to manage certificates

The Client application enables you to manage all your own certificates that are on the smart card you have open. To work with a certificate that is on another smart card, or receive a certificate on a different smart card, you must close down the Client application. Then restart it with the smart card you want to use.

Delete a certificate or a pending request

Note: This action cannot be undone easily, and sometimes not at all. Before you delete a certificate, or a request you have issued while managing your certificates, take the time to review its description. Then confirm that you want to delete the certificate or delete the request that affects it.

In the Smart Card View window:
1. Select the certificate or pending request you want to delete.
2. Open the Certificate menu and click Delete → Delete Certificate.
3. The Delete Certificate dialog is displayed. Page 40 describes the dialog.
4. Review the certificate description or the description of the pending request in the dialog. Page 42 describes the details you will see.
5. Click OK to confirm the deletion, or click Cancel if you change your mind.

Export a certificate from a smart card to a file

In the Smart Card View window:
1. Select the certificate you want to export from the open smart card.
2. Open the Certificate menu and click Export.
3. The Export Certificate dialog is displayed. Page 41 describes the dialog.
4. Select the type of encryption to use for encrypting the certificate.
5. Specify the location for creating a file to store the certificate. Either type the path and file name or click Browse to select the path and then type a file name.
6. Type a password to protect the file, and then type it again to confirm it. Use 8 to 32 alphanumeric characters.
7. Click OK, or click Cancel if you change your mind.

Import a certificate from a file to a smart card

In the Smart Card View window:
1. Select the certificate you want to import to the open smart card.
2. Open the Certificate menu and click Import.
3. The Import Certificate dialog is displayed. Page 41 describes the dialog.
4. Specify the current location of the file that contains the certificate. Either type the path and file name or click Browse to select them.
5. Supply the password you created when you exported the certificate to the file.
6. Type a descriptive name to identify the certificate on the smart card.
7. Click OK, or click Cancel if you change your mind.
Move a certificate to a different smart card

In the Smart Card View window:

1. Select the certificate you want to move from the open smart card to another smart card.
2. Follow the procedure to Export that certificate to a file. “Export a certificate from a smart card to a file” on page 18 describes the procedure.
3. Exit the Client application.
4. If you want to move the certificate to a physical smart card, load that smart card.
5. Restart the Client application and, this time, open that smart card. “Open a different smart card” on page 22 describes how to do this.
6. Follow the procedure to Import the certificate from the file to the open smart card. “Import a certificate from a file to a smart card” on page 18 describes the procedure.

Open a certificate to view details

In the Smart Card View window:

1. Select the certificate you want to view in more detail.
2. Open the Certificate menu and click Open.
3. The Open Certificate dialog is displayed. Page 42 describes the dialog.
4. Review the certificate description in the dialog.
5. Click OK when finished.

Suspend a certificate

In the Smart Card View window:

1. Select the certificate you want to suspend.
2. Open the Certificate menu and click Suspend.
3. The display contains information that identifies you and the certificate.
4. Examine the information to make sure that this is the certificate you want to suspend.
5. At RA’s URL, if the field is not already filled, select or type the URL of the Registration Authority that approved your original request for the certificate.
6. Click OK, or click Cancel if you change your mind.

Note: If you want to reactivate a suspended certificate, you must contact the RA Administrator before the certificate’s grace period expires. Once the grace period expires, a suspended certificate cannot be reactivated.

Renew a certificate

When you renew a certificate, the one you receive in its place will have a validity period of the same duration. You can either use the key pair from your old certificate or generate a new key pair.

In the Smart Card View window:

1. Select the certificate you want to renew.
2. Open the Certificate menu and click Renew.
3. The Renew Certificate dialog is displayed. Page 43 describes the dialog.

4. Review the certificate description in the dialog. The description includes the serial number and the issuer. Page 42 describes the details you will see.

5. At RA’s URL, if the field is not already filled, select or type the URL of the Registration Authority that approved your original request for the certificate.

6. If you do not want to use your old key pair, select a new algorithm and key size from the list of alternatives. All of those listed are suitable for your machine.

7. Click OK, or click Cancel if you change your mind.

Renew expiring certificates

Your organization has determined how early to warn you when a certificate is due to expire. The default is to warn you 30 days before expiration.

If any certificates on your open smart card will expire soon, the Certificate Renewal dialog displays them when you start the Client application. A table lists those certificates and has columns that summarize their descriptions. Page 42 describes the details you will see.

1. Examine the certificates. You can adjust the display if necessary:
   - Display more rows of the table by enlarging the window.
   - Resize a column to see more of the data.

2. Select the certificates that you want to renew and click OK.
   The Renew Certificate dialog is displayed for each certificate you selected. Page 39 describes the dialog.

3. For each certificate, complete the dialog and click OK.

   Note: If you do not select any certificates, the dialog is simply removed when you click OK.

Revoke a certificate

In the Smart Card View window:

1. Select the certificate you want to revoke.

2. Open the Certificate menu and click Revoke.

3. The Revoke Certificate dialog is displayed. Page 44 describes the dialog.

4. Review the certificate description in the dialog. Page 42 describes the details you will see.

5. At Reason for Revocation, select a reason for revoking the certificate. “Reasons for revoking a certificate” on page 36 lists the valid reasons.

6. At RA’s URL, if the field is not already filled, select or type the URL of the Registration Authority that approved your original request for the certificate.

   Note: You received this URL after you were preregistered and used it to claim your certificate.

7. Click OK, or click Cancel if you change your mind.
Sign a file

You can use a certificate to sign a file. When you sign a file with a digital signature, anyone who opens the file can tell whether the content has changed since you signed it. Note that signing does not encrypt the content of the file.

In the Smart Card View window:

1. Select the certificate you want to use to sign the file.
2. Open the Certificate menu and click Sign. The Sign a File dialog is displayed.
3. At Input File, specify the path and file name of the file you want to sign. Either type the path and file name or click Browse to select the file’s location.
4. At Output File, specify a path and file name for the signed file. Click Browse to select the path and file name instead of typing it.
5. At Signing Algorithm, select the algorithm you want to use to digitally sign the file. Page 44 describes the available choices.
6. If you want to view the file before you sign it, click View. This action launches the application associated with the file type of file being signed. For example, if you are signing an HTML file, the application launches your default browser to display the file.
7. Click OK to sign the file, or click Cancel if you change your mind.

Work with a list of certificates

In the Smart Card View window, the tabs display certificates by category:

- To see the list of your own certificates, click the My Certificates tab.
- To see the list of other certificates on the same smart card, click the Other Certificates tab. (There will not be other certificates unless you share the smart card with someone.)

A table displays basic information for each certificate.

- Scroll or resize the columns as necessary to view the information.
- Select a certificate, if desired.

Move between tabs

In the Smart Card View window, the tab that is currently displayed is brighter than the other one.

To move from one tab to the other, simply click the other tab.

Display more rows of a table

To display more rows of a table in a Client application window or in the Certificate Renewal dialog, you can do either of the following:

- Scroll the table to see additional rows.
- Enlarge the window or dialog to show more of the table.

Resize a table column

To resize a table column:

1. Place the cursor on the boundary of a column you want to resize.
2. Click the mouse and drag it left or right to change the column width.
3. Release the mouse button at the desired width.

Use the Client to manage smart cards

Topics in this section help you with the common tasks of smart card use and maintenance.

Open a different smart card

You open a smart card whenever you access the Client application. The default smart card is a virtual smart card. If you also have a physical smart card, your administrator can define it to the Client application for you.

To work with a different smart card from the one you specified at that time:

1. Exit the Client application
2. If you want to use your physical smart card, insert it.
3. Start the Client application again
4. On the splash screen, click OK.
   
   The Open Smart Card dialog is displayed. It contains a list of your smart cards that are defined to the Client application. Page 43 describes the dialog.
5. At Smart Card, select the smart card you want to open.
6. At Password, type your smart card password.
7. Click OK.
   
   The Smart Card View window is displayed.

Change a smart card password

Note: This dialog only enables you to change the password for a virtual smart card you have open. If you have a physical smart card, see the documentation that came with the smart card. It will provide directions for changing the password.

In the Smart Card View window:

1. Open the Smart card menu and click Change Password.
   
   The Change Password dialog is displayed. Page 44 describes the dialog.
2. Type the current password for your virtual smart card.
3. Type your new password, and then type it again to confirm it. Use 8 to 32 alphanumeric characters, but make it easy to remember.
   
   Note: Passwords are not displayed as you type.
4. Click OK, or click Cancel if you change your mind.

View smart card properties

In the Smart Card View window:

1. Open the Smart card menu and click View Properties.
   
   The Smart Card Properties dialog is displayed. Page 45 describes the dialog.
2. Review the smart card description in the dialog.
3. Click OK when finished.
Exit the Client application

To exit the Client application:

1. If you have a dialog open, either complete the dialog and click **OK**, or else click **Cancel**.
2. In the **Smart Card View window**, open the **Smart card** menu and click **Exit**.

Uninstall the Client application

Use the following procedure if you need to remove the Trust Authority Client application from your workstation.

1. Select **Start** → **Settings** → **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Select the **IBM SecureWay Trust Authority Client** program folder, and click **Add/Remove**.
4. When prompted to confirm that you want to delete the program, click **Yes**.
5. If you see a message about certain folders not being deleted, click **Details**. You must manually delete any folders listed in the Details window to completely remove the Client application from your system.

**Note:** If you are unable to uninstall the Client application, try re-booting the system. That should free up shared files and allow you to delete them. If you are still unable to use the Windows **Add/Remove Programs** menu to uninstall the application, you may need to manually edit the Windows Registry to remove the Client entries.
Tell me about...

The topics in this section define or describe concepts that are related to enrollment, registration, certification, certificates, and access to secure resources.

Enrollment

Enrollment is applying for a certificate. Trust Authority offers more than one method of enrollment, and your organization’s policies dictate which methods are available. You can access enrollment forms through your Web browser when you need to request a certificate. On the enrollment Web page, you can link to, complete, and submit an enrollment form. Your purpose might be any of the following:

- To request a **CA certificate** in preparation for your enrollment tasks.
- To request a **browser certificate** for yourself.
- To request a certificate for a specific **server or device**.
- To **preregister** yourself or someone else for a certificate to access a PKIX-compliant application.

Later that person can receive the certificate by supplying appropriate information to the Trust Authority Client application on their workstation.

Data from enrollment forms goes into **database records** that Registration Authority (RA) registrars can view from the Trust Authority Registration Authority Desktop (RA Desktop).

Preregistration

Trust Authority enables a program or an administrator to preregister prospective users.

If you preregister other people for certificates, here is the scenario for doing so:

- You need to get information about the person you want to preregister. You might get it from the person or use organization records, such as information from a database.
- You access the enrollment page from your **Web browser**. There is an **enrollment form** especially for preregistering someone.
- You complete the form, supplying information that describes the person and the type of certificate they want. Then you submit the form.
- You check on the status of the request.

When the preregistration request is approved, you receive a transaction ID, password, and the URL of the RA that approved the request.
You give this information—by telephone, e-mail, or in person—to the person you preregistered. Optionally, for their convenience, you can give them a preregistration file that contains other request information. The person uses what you send when they are ready to request their certificate.

If you are a user who has been preregistered, here is the scenario for getting your certificate:

- By telephone, by e-mail, or in person, you receive the information you need to claim your certificate. You will either get a transaction ID, a password, and the URL of the RA that approved the request, or else you will get a preregistration file and password.
- You use the Client application to request your certificate. When prompted, you supply the information you received.
- During processing of your certificate request, the request appears in the Client application window, along with any certificates you already have on the open smart card.
- When the certificate is ready, it arrives through the Client application. The Client application automatically stores it on your smart card. The display indicates that you have the certificate.

Web browser support

Trust Authority enables you to create an enrollment request by completing and submitting an enrollment form through either of the following Web browsers:

- Microsoft Internet Explorer, release 4.0 or later.
- Netscape Navigator or Communicator, version 3.0 or later.

Registration

Registration is the process of granting a digital certificate to a person or other entity. In Trust Authority, preliminary to registration, either a program or an registrar evaluates the information that was provided with the enrollment request. Then, whether or not the request is granted, the Trust Authority RA creates a record for the request in the registration database. If the decision is to grant the certificate, the Trust Authority Certificate Authority (CA) issues the certificate.

Business policy

When a program or an registrar evaluates your enrollment information, they apply the business policies of your organization to some of the enrollment information. The type of information a program can evaluate is less complex than the kind a registrar evaluates. Values tend to be precise, such as the minimum number of years in a residence. Trust Authority enables your organization to provide policy information to such a program. The program uses this information in its evaluations.

Registration authorities

In Trust Authority, the RA is a server application. It is responsible for some of the administrative tasks necessary to the registration of users, including:

- Confirming a user’s identity
- Verifying that a requester is entitled to a certificate with the requested attributes and permissions
- Approving or rejecting requests to create or revoke certificates
Suspending or reactivating certificates

Verifying that someone who attempts to access a secure application has the private key associated with the public key within a certificate

Registration databases

A Trust Authority registration database stores registration records. The registration database is a relational database, created with IBM DB2 Universal Database. Trust Authority encrypts the records. However, through the RA Desktop an authorized registrar can read most of the registration information.

Registration domains

Each Trust Authority system has a single registration domain. This domain defines the business policies, certificate policies, and resources that are associated with registration and certification at your organization. Users who want to access a resource must be registered for the domain for that resource.

When the RA server software is installed, it contains the framework that allows an organization to set up the registration facility. It can use any of the languages or policies that the Registration Authority supports. The domain name, language, and installation path form the URL for accessing a given instance of the registration facility.

For example, if your public Web server name is MyPublicWebServer, and your registration domain name is MyDomain, you would use the following URL to access the registration facility:

http://MyPublicWebServer/MyDomain/index.jsp

A Trust Authority system includes a default Java Server Page (index.jsp) with the registration facility. That page is displayed at the enrollment URL for your registration domain. It provides the following types of enrollment services:

- Prospective users go to that Web page to request a certificate, and to renew or revoke their own browser certificates.
- Administrators may also visit the enrollment Web page to preregister other users.

Trust Authority registrars access the RA Desktop to work with the registration requests and certificates that are associated with a registration domain.

Registration records

Each request for a certificate is an enrollment form that is submitted to the Trust Authority RA. Each enrollment request results in a registration database record. Updates to this record reflect every action on the request, even a rejection of the request. If a certificate is created, the same record reflects any events that relate to that certificate. Thus the registration record contains all the events in the life cycle of the request and the associated certificate.

Record attributes

The attributes of a record in the registration database are variables that describe the enrollment request. For fulfilled requests, the variables also describe the certificate that was granted. Other attributes are processing variables that help your organization enforce its business policies. Many attributes and their values are visible to registrars through the RA Desktop.
Certification

Certification is the creation of a digital certificate for an entity or person. For Trust Authority, certification occurs only after evaluation and approval of an enrollment request. As the result of registration, the Certificate Authority (CA) issues the certificates. For Trust Authority, the type of certificate that is issued is consistent with the business policies of your organization.

Certificate authorities

In Trust Authority, the CA is a server program responsible for issuing digital certificates in accordance with the policies of your organization.

Trust Authority supports cross-certification, in which CAs that trust each other agree to accept each other’s certificates as proof of authenticity. Trust Authority also supports a CA hierarchy. CAs trust the CAs that are above them in the hierarchy and accept the certificates of those CAs as proof of authenticity.

Certificate revocation lists

The Trust Authority RA publishes a certificate revocation list (CRL) at regular intervals. This lists the certificates that are no longer valid, so that holders who present them are not authenticated.

Any CA, RA, or application can access this list to determine whether a certificate has been revoked. This is one way that the Trust Authority RA provides security when users try to access the secure applications of your organization.

Directories

The Directory that Trust Authority uses for storing certificates is the IBM SecureWay Directory. This Directory may be one that your organization set up specifically for use with Trust Authority. Alternatively, it may be one that you have installed previously and use with other applications.

The protocol that Trust Authority uses for accessing the Directory is the Lightweight Directory Access Protocol (LDAP).

Distinguished names

The distinguished name (DN) is an element of the Directory entry for a digital certificate. It uniquely identifies the position of the entry in the hierarchical structure of the Directory.

Certificates

A certificate is a digital credential, signed by a CA, that vouches for the identity of the certificate holder. The holder can use the certificate as authentication when communicating with others or when requesting access to a secure application. In Trust Authority, even servers, applications, and devices such as printers and smart cards must have certificates, to authenticate them to users and to each other.

Trust Authority supports X.509v3 certificates in the following categories:
- Browser certificates
- Server certificates
- Device certificates
- Certificates for accessing PKIX-compliant applications
- Cross-certificates for CAs
Trust Authority also supports the following protocols:

- SSL
- S/MIME
- IPSec
- PKIX CMP

A default Trust Authority installation provides a variety of certificate types that are based on these categories and protocols. Enrollees can request certificates that meet their needs. “Supplied certificate types” on page 35 describes the certificate types.

**Browser certificates**

A browser certificate is a digital credential that is typically stored in an encrypted file by your Web browser. Some applications permit you to store the keys on a smart card or other media. In a Trust Authority system, you can request a browser certificate directly through your Web browser. Later, if necessary, you can return to the enrollment Web page to renew or revoke that certificate.

**CA certificates**

Every browser, server, device, or application that has a certificate to present to Trust Authority servers must also have a compatible CA certificate. This certificate is needed for authenticating communications from servers that hold certificates issued by the Trust Authority CA.

You must have a Trust Authority CA certificate in your browser to use the secure Trust Authority enrollment services. You can get this the first time you visit the Trust Authority enrollment Web pages. After that, whenever you request a certificate from the enrollment services, you can download a corresponding CA certificate that is compatible with it.

For example, if you request a 2-year SSL browser certificate, you can receive a CA certificate that is compatible with that certificate.

**Note:** Early releases of Netscape could accept a site certificate presented by a Trust Authority server. That certificate was acceptable for both server-authenticated and client-authenticated communications with that server. However, the latest release of Netscape requires a CA certificate for client-authenticated sessions.

**Server or device certificates**

If it is part of your job, you can request a certificate for a server or a device. Use the enrollment form that is provided through your Web browser.

The server or device for which you are requesting a certificate must use the PKCS #10 request format.

**Certificate extensions**

Certificate extensions are optional elements in the format of an X.509v3 certificate. Extensions make it possible to incorporate additional fields into the certificate. Trust Authority provides a group of certificate extensions to enable your organization to customize the certificates it issues. These additional fields are known as business process variables.

**Certificate life cycles**

When you request a certificate, you initiate a life cycle that continues for the lifetime of that credential. That life cycle ends when the certificate is revoked or when it expires.
If a certificate is renewed, a new record is created in the registration database.

**Renewability**

The renewability of a certificate is one of the characteristics that an registrar can change for you from the RA Desktop:

- If your certificate is renewable, you can apply for a new one while the old one is still valid. Possession of a renewable certificate simplifies the enrollment process and the registration effort.
  - If you have a renewable browser certificate, you can request renewal on the enrollment Web page.
  - If you have a renewable certificate for accessing a PKIX-compliant application, you can request renewal by using the Client application.
- If your certificate is non-renewable, you must wait until it expires, and then enroll again if you still need a certificate. When you enroll, you must supply all the information, as if you were registering for the first time.

**Access to secure resources**

The topics in this section relate to the use and administration of certificates.

**Access control**

An access control list (ACL) authenticates and authorizes internal Trust Authority users, devices, and software. For example, the RA Desktop support servlet uses the ACL to authenticate and authorize registrars before they can access the RA Desktop.

**Authentication and authorization**

Authentication provides proof of identity, whereas authorization provides permission to do something. Trust Authority enables your organization to insist on both before users access secure applications. In turn, certificate holders can be confident that the applications they are using are secure.

**Digital signatures**

By using one of your certificates, you can sign a file with a digital signature. This tells whoever opens the file whether the content has changed since you signed it. Signing does not encrypt the content of the file.

**Smart cards**

Smart cards are storage devices for keeping digital credentials secure. There are virtual smart cards, which reside on your workstation, and physical smart cards, which are either internal or external. You can take an external smart card from machine to machine, but it is less secure due to its portability.

When you receive a new certificate using the Client application, your certificate is stored automatically on the smart card that you have open.

**Key backup and recovery facility**

Trust Authority 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 request, 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 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.
The topics in this section include field descriptions, valid field values, and the meanings of certificate attributes. It also includes information that may help you if you are using Trust Authority in a language other than English.

Web page enrollment form

The enrollment form has sections for describing the prospective certificate holder and for describing the certificate request. Some fields in the sections are present only for a specific type of enrollment.

Note: If your organization customizes the enrollment forms, the content may differ somewhat from what is in this guide.

Registration Information includes the following fields, where appropriate to the type of certificate request:

Type of Certificate
Select a value from the list. “Supplied certificate types” on page 35 describes the certificate types that are supplied with a default installation.

First Name
Your first name or given name. Include a middle name or initial, if desired.
For preregistration, this refers to the person you are preregistering.

Last Name
Your last name, family name, or surname.
For preregistration, this refers to the person you are preregistering.

E-mail Address
Your e-mail address, including the at sign (@) and any periods (.). Some certificate types require this address, such as certificates for secure e-mail. To select E-mail Notification, you must supply an e-mail address.

E-mail Notification
Select this option to receive an e-mail notification about the outcome of this enrollment request.

Note: If the RA server is installed on a Windows NT platform in your organization, the registration facility’s configuration file (raconfig.cfg) may need to be updated to point to an SMTP host to enable this feature. For details, see the Trust Authority Customization Guide.
Challenge Question
A question that is special to you, that can be used to authenticate your identity or prevent someone from masquerading as you. You are asked this question when you check the status of the enrollment request. You must answer the challenge question whether the request is for yourself, for a server or device, or to preregister someone.

Challenge Response
A response to the challenge question you supplied. Provide a response that is easy to remember. You must provide the same response when you check your the status of your request.

Note: The response is case-sensitive.

Password
*(preregistration only)* The password that the person you are preregistering must provide to the Client application when they are ready to download the certificate. Use the characters A-Z, a-z, and 0–9. The password can have from 8 to 32 characters.

If you do not supply a password, the registration facility generates a 10-character password for you. On approval of the preregistration request, you receive it along with a transaction ID.

Confirm Password
*(preregistration only)* Type the same password again.

Certificate Request Information includes the following fields:

PKCS #10 Certificate Request
*(Server or device enrollment only)* The content of the PKCS #10 certificate request generated by your server or the device for which you are requesting a certificate. If the request was saved in a file, open the file in a text editor such as Windows Notepad. Copy the content and paste it in the text box on the enrollment form.

Common Name
A name to identify this certificate.
- For a person, typically this is the person’s full name.
- For a server or device, it is usually the host name. You must supply this value if there is no host name in the PKCS #10 Certificate Request field.

Key Size
*(Netscape browser enrollment only)* The key size for your public/private key pair. Select a value. Larger keys are more secure, but they also increase the time that is needed for connecting to a secure session.

Cryptographic Service Provider
*(Internet Explorer browser enrollment only)* The Cryptographic Service Provider to generate your public/private key pair. Select a value. Larger keys are more secure, but they also increase the time that is needed for connecting to a secure session.

The default is Microsoft Base Cryptographic Provider, which provides 512–bit key encryption.

If installed in your system, the Microsoft Enhanced Cryptographic Provider provides 1024–bit key encryption.
Key Set

(*Internet Explorer browser enrollment only*) The key pair to use. Select **Generate New Key Set** or open the list and select one of your existing key pairs.

**New Key Set Name**

(*Internet Explorer browser enrollment only*) The name for the new key pair to be generated. You can leave this blank and have a Globally Unique Identifier (GUID) generated for the name, but these make the key pair harder to recognize.

**Additional Security Options**

Additional security that Microsoft Internet Explorer offers for your new key pair. If you select this option, your Web browser displays Internet Explorer dialogs for setting these options immediately after you submit this enrollment form.

**Organization Name**

The legally registered name of your organization

**Organizational Unit**

The name of your division or department, such as Human Resources or Software Development.

**Street Address**

The street address of your organization

**Locality**

The city or municipality where your organization is located, such as Chicago or Paris.

**State or Province**

The state or province where your organization is located. Whether you spell out the full name of the state or province, or use a standard abbreviation, depends on your registration policies. For example, use either New York or NY.

**Country**

The country where your organization is located. Select a value.

**Domain Name**

The host name of the machine where a certificate will be installed. This field is optional for server certificates and end-user certificates (browser certificates and certificates obtained through pre-registration for the Trust Authority Client application). If you choose to include it, you must identify the machine where the browser, Client, or Web server is installed. For IPSec certificates, you must identify the IPSec device where the certificate will be installed.

**Supplied certificate types**

A Trust Authority system provides multiple certificate types for the supported certificate categories and protocols. Variations include different validity periods. The name of the certificate is an indicator of how long it is valid and the primary use of the key. See the **Glossary** for descriptions of the various features.

**CA Cross-certificate**

Enables the CA that holds it to have its certificates trusted by the issuing CA. The certificate provides digital signature and non-repudiation.

**1– and 2–year Data Encipherment**

Enables the holder to encrypt data. The certificate is not intended for other purposes.
1- and 2-year E-mail Protection
Enables the holder to use the Secure Multi-Purpose Internet Mail Exchange (S/MIME) protocol. This protocol protects e-mail or other mime objects. It provides authentication of origin, message integrity, non-repudiation of origin, and confidentiality. It is a typical choice for an end user.

1- and 2-year IPSec
Assures the integrity and confidentiality of data that is sent over the internet in Internet protocol packets. An IPSec certificate is for data rather than users, and is often assigned to a router.

1- and 2-year Key Encipherment Only
Enables the holder to encrypt keys. The certificate is not intended for other purposes.

1- and 2-year Non-repudiation
Provides message encryption and digital signing capabilities, to prevent non-repudiation of the origin of a message or non-repudiation of its delivery.

1- and 2-year Signing Only
Enables the holder to sign a file digitally. The certificate is not intended for other purposes.

1- and 2-year Web Client Authentication
Enables a Web browser to participate in a client-authenticated SSL session. With this certificate, the user of the browser can access a specific secure Web site. The certificate provides digital signature, non-repudiation, and key encipherment. It is a typical choice for an end user.

1- and 2-year Web Server Authentication
Enables a server to participate in a server-authenticated SSL session. The certificate provides digital signature and key encipherment.

Enrollees or people who preregister for someone else can request a suitable certificate type. Enrollment forms list the available certificate types in the Type of Certificate field. In the Client application, the Purpose field of a certificate description lists the certificate type.

Note: The list you see might not match this list. Your organization might have changed the names or even the offerings.

Reasons for revoking a certificate
When you revoke a certificate, you must select a reason for doing so. The following are valid reasons you can select when you revoke a certificate:

CA key was compromised
The key of the Certificate Authority that issued the certificate was compromised.

Certificate was superseded
You have a new certificate and no longer need this one.

No reason
You are not specifying a reason.

Original use no longer valid
You no longer need the certificate for its original use. For example, you no longer need to access the resource or application for which the certificate was issued.
User changed affiliation
You are no longer affiliated with the organization to which the certificate applies.

User key was compromised
Your private key was compromised.

Note: The enrollment forms list the valid reasons in the Reason field when you revoke a certificate on the enrollment Web page. The Client application lists them in the Reason for Revocation field of the Revoke Certificate dialog. Page 20 describes the dialog.

System requirements for browser enrollment
IBM recommends the following workstation configuration for using the browser enrollment forms provided with the registration facility.

- The following physical machine setup:
  - 166 MHz Intel 486 processor with 32 MB of RAM, at a minimum
    (200 MHz Intel Pentium® processor with at least 64 MB of RAM is preferred)
  - A computer display that supports VGA resolution, or better

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

- One of the following Web browsers:
  - Netscape Navigator or Netscape Communicator, version 4.05 or later
  - Microsoft Internet Explorer, version 5.0, with Java enabled

- Optionally, support for a physical smart card. If you plan to store certificates on smart cards, you may need to upgrade your browser to a version required by that smart card. For example, the IBM SecureWay Smart Card Security Kit requires one of the following browsers:
  - Netscape Navigator or Netscape Communicator, version 4.6 or later
  - Microsoft Internet Explorer, version 5.0 or later

System requirements for the Client application

- You must install the Trust Authority Client application on a Windows NT machine.

- You cannot install the Client application on the same machine where the Trust Authority server programs were installed. An administrator should install the installation image as part of installing Trust Authority on the server, but not run it on the same machine.

- To install the Client application, you must have a minimum of 80 MB free space on the hard drive where your temporary files are placed. To determine which drive this is, enter the following command to check your environment settings for the TEMP variable:

  `md %temp%`

  If a temp directory exists, the system displays the message "A subdirectory or file drive:\TEMP already exists". Otherwise, the system creates the temp directory. Note that the installation program removes temporary files that it creates after the Client application has been installed.
You must also have 60 MB free space on the hard drive where you choose to install the
Client application, and 0.5 MB free space on the hard drive where the Windows
operating system is installed.

To use a physical smart card with the Trust Authority Client application, you must use a
browser version that is supported by your smart card. For example, the IBM SecureWay
Smart Card Security Kit can be used with the following browsers:

- Microsoft Internet Explorer, version 5.0 or later
- Netscape Navigator or Netscape Communicator, version 4.6 or later

**Client application main window**

All the major functions of the Client application are available in the Trust Authority: **Smart
Card View** window.

**Menus in the Smart Card View window**

The following menu options are available from the Smart Card View window. Many of the
options require that you first select a certificate from the **table** on the two **tabs** below the
menu. To select a certificate, click its row in the table.

**Smart Card menu**

- **Change Password**
  Change the password of the open smart card.

- **View Properties**
  View the properties of the open smart card.

- **Exit**
  Close down the Client application.

**Certificate menu**

- **New**
  Request a new certificate by using your preregistration data:
  - A **transaction ID**
  - A **preregistration file**

- **Open**
  View information about the selected certificate.

- **Import**
  Import the selected certificate to a smart card.

- **Export**
  Export the selected certificate from a smart card.

- **Delete**
  Delete the selected certificate from a smart card.

- **Renew**
  Renew the selected certificate.

- **Revoke**
  Revoke the selected certificate.

- **Sign**
  Use the selected certificate to digitally sign a file.

- **Help**
  Links to help for the current window.
Help Topics
Displays the Trust Authority User’s Guide.

About Displays information about the Client application.

Tabs in the Smart Card View window
Below its menu bar, the window has two tabs:

My Certificates tab
Displays a table that lists all your current certificates on the open smart card, and your pending requests, such as new certificate requests and revocation requests.

Other Certificates tab
Displays a table that lists certificates that are on the same open smart card, but do not belong to you.

Tables in the Smart Card View window
Each tab of the Smart Card View window contains a table that describes certificates on the smart card. Each row describes a single certificate. The columns provide the following information:

Status The status of the certificate or of the request for a certificate. Values include the following:
- Issued The RA issued the certificate, and the Client application stored it on the smart card.
- Rejected The RA rejected the certificate request.
- Renewal Submitted The renewal request has been sent to the RA.
- Revocation Submitted The revocation request has been sent to the RA.
- Submitted The certificate request has been sent to the RA.

Label A unique description given to the issued certificate.

Subject Name The distinguished name of the certificate.

Purpose The primary use of the certificate.

Expiration Date The date that the certificate is no longer valid.

Client application dialogs
The Client application provides dialogs where you can specify details as you work with your certificates. You begin each task from the menus of the Smart Card View window, and the Client application displays the appropriate dialog for the task.

Certificate Renewal dialog
On this dialog, you can see summary information for each certificate that is due to expire within the interval that your organization sets. The default is 30 days. The table in the dialog
has a row for each expiring certificate.

Columns provide the following information:

**Label**
A unique description given to the issued certificate.

**Serial Number**
The serial number of the certificate.

**Purpose**
The primary use of the certificate. This field contains a certificate type. "Supplied certificate types" on page 35 lists the supported types for a default installation.

**Expiration Date**
The last date the certificate is valid.

To renew one or more of these certificates, examine the summary information, select the certificates, and click **OK**. If you select nothing, clicking OK simply closes the dialog.

Related topics:

"Display more rows of a table" on page 21
"Resize a table column" on page 21

**Change Password dialog**
On this dialog, you can change your password for a virtual smart card.

**Note:** To change the password for a physical smart card, you must use the software that was provided with the smart card.

**Current Password**
Type the current password for your virtual smart card.

**New Password**
Type the new password you want to use. You can specify from 8 to 32 characters, using A-Z, a-z, and 0–9.

**Confirm Password**
Retype the same new password.

**Delete Certificate dialog**
On this dialog, you can review summary information for one of the following that you selected for deletion:

- A certificate that you want to delete from the open smart card.
- A pending request that you submitted but that you want to cancel before the RA processes it. The pending request could be of any kind. It could even be a request to delete or revoke a certificate.

1. Examine the information that describes the certificate or request. Page 42 describes the details you will see.
2. If you still want to delete the item, click **OK**.

**Note:** If the pending request you wanted to delete is not displayed, it is no longer pending, and it is too late to delete it.
Export Certificate dialog

On this dialog, you supply the information that is needed for exporting a certificate from the open smart card to a file.

**Type of Encryption**
Select the level of encryption for the file. Stronger encryption requires a larger key and takes longer to create a secure connection.

**File Name**
Specify the path and file name for storing the certificate when you export it from your smart card. The **Browse** button enables you to select the path before you type the file name.

**File Password**
Protect the file by specifying a password for it. You can use 8 to 32 alphanumeric characters (A-Z, a-z, 0-9).

Import Certificate dialog

On this dialog, you supply the information that is needed for importing a certificate from a file to the open smart card.

**File Name**
Specify the path and file name of the file that contains the certificate. The **Browse** button enables you to select the path and file name instead of typing it.

**File Password**
Specify the password that protects the file.

New Certificate Using a Preregistration File dialog

On this dialog, you can enroll for a certificate by specifying a preregistration file and password that you received from the administrator who preregistered you. You may have received them through e-mail or on a diskette.

**Preregistration File Name**
Specify the path and file name of the preregistration file you received. The **Browse** button enables you to select the path and file name instead of typing it.

**Password**
Type the password you received for claiming your certificate.

At your organization’s option, after you enter your password, you may see a display of attributes and values associated with your certificate request. Some of these may be editable.

New Certificate Using a Transaction ID dialog

On this dialog, you can enroll for a certificate by using transaction information that you received from the administrator who preregistered you. You may have received this information through e-mail or in a phone call.

**Transaction ID**
Type the transaction ID you received for creating the new certificate.

**Password**
Type the password you received for claiming the certificate.
RA’s URL
From the list, select the URL that matches the one you received, or type it in the text box. For example, pkix://<your server>:<your port> where <your server> is the hostname of your RA, and <your port> is the port on which that URL can be accessed.

Key Algorithm
Select the encryption algorithm your organization has suggested that you use for the private key that is associated with this certificate. The values on the list are suitable for your machine. Along with Key Size, this algorithm defines the strength of the key.

Key Size
Select a size for the private key that is associated with this certificate. The values on the list are suitable for your machine. Longer keys are more secure, but they also increase the time that is needed for connecting to a secure session.

Open Certificate dialog
On this dialog, you can view the details of the certificate or certificate request you selected in the Smart Card View window.

The description is divided into sections. The sections include general information, subject information, and issuer information. The information for a certificate request is somewhat different from that of a certificate. For example, a certificate request has no serial number.

General Information includes the following:

Label
A unique description given to the issued certificate.

Serial Number
The serial number of the certificate.

Status
The status of the certificate or certificate request.

Effective Date
The date the certificate becomes valid.

Purpose
The primary use of the certificate.

Key Algorithm
The identifier of the encryption algorithm for the private key associated with the certificate. Along with the Key Size, this algorithm defines the strength of the key.

Key Size
The length of the private key associated with the certificate.

E-mail Address
Your Internet e-mail address.

Subject Information includes the following information about the entity to which the certificate was issued:

Common Name
The name of the certificate holder.

Organizational Unit
The business unit the certificate holder belongs to.
Organization Name
The certificate holder’s organization.

Locality
The state or province of the certificate holder.

Country
The country of the certificate holder.

Issuer Information includes the following information about the CA that issued the certificate:

Common Name
The identity of the CA that issued the certificate.

Organizational Unit
The business unit the issuer belongs to.

Organization Name
The name of the issuer’s organization.

Locality
The issuer’s state or province.

Country
The issuer’s country.

Open Smart Card dialog
On this dialog, you select from a list the smart card you want to use with the Client application.

Smart Card
Select a smart card from the list.

Password
Type the password for the smart card you selected.

Renew Certificate dialog
On this dialog, you can review summary information for a certificate to ensure that you want to renew it.

If you decide to renew the certificate, the one you receive in its place will have a validity period of the same duration. You can either use the key pair from your old certificate or generate a new key pair.

To continue with the renewal, supply the following:

RA’s URL
If the field is not prefilled, either select the URL of the RA that approved the original certificate request, or type it in the text box. If you do not know the URL, contact your registration domain administrator.

Key Algorithm
To use the key pair from your expiring certificate, ignore this field. To generate a new key pair, select a value. The values on the list are suitable for your machine.

This is the encryption algorithm for the private key that is associated with this certificate. Along with Key Size, this algorithm defines the strength of the key.
Key Size
To use the key pair from your expiring certificate, ignore this field. To generate a new key pair, select a value. The values on the list are suitable for your machine.

This is the size for the private key that is associated with this certificate. Longer keys are more secure, but they also increase the time that is needed for connecting to a secure session.

Revoke Certificate dialog
On this dialog, you can review summary information for a certificate to ensure that you want to revoke it.

To continue with the revocation, supply the following:

RA’s URL
If the field is not prefilled, either select the URL of the RA that approved the original certificate request, or type it in the text box. If you do not know the URL, contact your registration domain administrator.

Reason for Revocation
Select from the following to identify the reason you want to revoke the certificate.

- User key was compromised
- CA Key was compromised
- User changed affiliation
- Certificate was superseded
- Original use no longer valid
- No longer used

“Reasons for revoking a certificate” on page 36 defines these reasons.

Sign a File dialog
On this dialog, you can use a certificate to sign a file. When you sign a file with a digital signature, anyone who opens the file can tell whether the content has changed since you signed it.

Input File
Specify the path and file name of the file you want to sign. The Browse button enables you to select the path and file name instead of typing it.

Output File
Specify the path and file name for the file after it has been signed. The Browse button enables you to select the path and file name instead of typing it.

Signing Algorithm
Select the algorithm you want to use to sign the file:

SHA1 With RSA
Generates a signature by applying a secure hash algorithm (SHA-1) to the signature calculation defined in the RSA (Rivest, Shamir, and Adleman) standard. With RSA, verification of the signature is relatively fast. However, generation of the signature may take longer than when using other algorithms.
MD5 With RSA
Generates a signature by applying the MD5 message digest function to the signature calculation defined in the RSA standard. The MD5 algorithm is faster than SHA-1. However, SHA-1 creates a larger message digest which may result in a more tamper-resistant signature.

Click View if you want to view the file before you sign it. This action launches the application associated with the file type of file being signed.

**Smart Card Properties dialog**
On this dialog, you can review information about the open smart card.

**Smart Card**
The name of the smart card.

**PKCS #11 Version**
The level of PKCS #11 encryption.

**CDSA Version**
The level of Common Data Security Architecture the smart card is designed to use during cryptographic and data storage operations. You cannot use this smart card with smart card software that runs an earlier version of CDSA than the one listed.

**Space left on Smart Card**
The amount of space left for storing certificates and certificate requests.

**Help for the Client application**
The Client application provides the following kinds of help:

- The Smart Card View window has a Help menu that contains the following:
  - Help Topics
    Displays the Trust Authority User’s Guide.
  - Help for this Window
    Displays help for the current window.

- Each dialog has a Help button that provides help specific to your task.
- Each field has context-sensitive help, which you see when your cursor moves over the field.

**Related topics:**

"Move between tabs" on page 21

**National language considerations**
This section summarizes the differences between the English version of Trust Authority and the other languages that it supports. If you request or manage certificates using a non-English version of Trust Authority, review this section to learn about differences in how information may be displayed or processed in your language.

Listed below are the language codes for the supported languages.

- de_DE for German
- en_US for English
- es_ES for Spanish
Requesting certificates that have non-ASCII DNs

You can use Trust Authority to request certificates that contain non-ASCII distinguished names (DNs), such as a certificate that uses accented characters for the common name. The DN of the certificates created by Trust Authority are encoded in Printable, Teletex (T.61), or UTF-8 characters. Typically, DNs that contain European-accented characters are encoded in Teletex and DNs that contain native characters in Chinese, Japanese, or Korean are encoded in UTF-8. Depending on your browser type and how it was localized for your environment, it may not render these certificates correctly when you view them.

Using Netscape with certificates that have non-ASCII DNs

The Netscape browser cannot handle UTF-8–encoded certificates. Trust Authority encodes DNs that contain double-byte characters (Chinese, Japanese, or Korean) in UTF-8. Because the currently available versions of Netscape cannot handle UTF-8–encoded certificates, you cannot use Netscape to request certificates or to import certificates that contain Chinese, Japanese, or Korean characters in the DN. Instead, use Microsoft Internet Explorer to request certificates in these languages.

Using Netscape to display the key size

When using Netscape and a non-English version of the browser enrollment form, the Key Size field displays unrecognizable text as squares ([ ] [ ] [ ]). This text is generated internally by the browser, which is not in UTF-8 format. The Netscape browser generates this string of text only in native character sets (such as ISO-8859-1 for English and Western European languages, Big5 for Traditional Chinese, and BG2312 for Simplified Chinese).

Because the enrollment JSP pages are encoded in UTF-8, the browser fails to recognize the string in its native character set. Therefore, this string cannot be displayed using the UTF-8 font set in the browser.

The choices for Key Size in a U.S. domestic version of the Netscape browser are as follows:

- 1024 (High Grade)
- 768 (Medium Grade)
- 512 (Low Grade)

Because of government export restrictions, a non-English version of the browser is likely to have only one entry with a low grade, 512-bit key size.

Accessing Client application message files

After installing the Trust Authority Client application, you must update the NLSPATH environment variable, as follows:

From: C:\Program Files\IBM\TrustAuthority\msg\%L\%N
To: C:\Program Files\IBM\TrustAuthority\TACLIENT\msg\%L\%N
This change enables you to receive error messages in the correct language.
Notices

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 NON-INFRINGEMENT, 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.
Licenses 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 or Tivoli Systems, Inc. in the United States, or other countries, or both:

IBM
AIX
AIX/6000
DB2
DB2 Universal Database
SecureWay
Tivoli
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.
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 on 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.
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.

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

Data Encryption Standard (DES)
An encryption block cipher, defined and endorsed by the U.S. government in 1977 as an official standard. 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.

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.

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

hierarchy
The organization of Certificate Authorities (CA) in a trust chain, starting with the self-signed CA or root of roots at the top, and ending with the CA that issues certificates to end users.

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.

**J**

**Java**

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

**Java applet**

*See applet. Contrast with Java application.*

**Java application**

A stand-alone program 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 Backup and Recovery**

This feature of Trust Authority enables you to backup and recover the end entity certificates and their corresponding public and private keys certified by Trust Authority. The certificate and keys are stored in a PKCS #12 file. This file is protected by a password. The password is set at the time the certificate and keys are backed up.

**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.*

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 on-line 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.

S

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 government) 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.

T

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 chain
A set of certificates that consists of the trusted hierarchy from the user certificate to the root or self-signed certificate.

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.

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.
Index

A
access control list 30
algorithms for signing 44
attributes, database record 27
authentication 30

B
backup and recovery, key 30
backup request, issuing key 13
browser certificate 29
browser certificate request 6
browser requirements 37
browser support 26
business policy 26
business process variables 29

certificate management (from Client) 18 (continued)
  viewing a list 21
  viewing details 19
certificate management (on Web) 10
  preregistering 8
  renewing 11
  requesting for browser 6
  requesting for server or device 7
  revoking 12
  suspending 11
Certificate Renewal dialog 39
certificate revocation list 28
certificate types 35
certification 28
  cross-certification 28
  hierarchy 28
Challenge Response 6, 7, 8, 10, 33
Change Password dialog 40
Client application 3
  accessing 16
  enabling a physical smart card 15
  enrollment 17
  exiting 23
  installing 14
  managing certificates 18
  scenario for getting certificate 25
  system requirements 37
  uninstalling 23
Client application dialog 39
Certificate Renewal 39
Change Password 40
Delete Certificate 40
Export Certificate 41
Import Certificate 41
New Certificate Using a Preregistration File 41
New Certificate Using a Transaction ID 41
Open Certificate 42
Open Smart Card 43
Renew Certificate 43
Revoke Certificate 44
Sign a File 44
Smart Card Properties 45
Client application enrollment 17
  with preregistration file 17
  with transaction ID 17
Client application request, deleting 18
Client application window elements 38
compromised key 36
cross-certification 28

C
CA certificate 5, 29
CA hierarchy 28
certificate 28
  backing up 13
  categories 28
  database records 27
  deleting 18
  details 19
  expiring 20, 39
  exporting to a file 18
  for using enrollment services 5, 29
  importing from a file 18
  managing from Client application 18
  managing from enrollment Web page 10
  non-renewable 30
  recovering 13
  renewable 29, 30
  requesting from Client application 17
  requesting from enrollment Web page 5
  summary information 21
  types 35
Certificate Authority 3, 28
certificate extensions 29
certificate life cycle 27, 29
certificate management (from Client) 18
  moving to a different smart card 19
  opening 19
  renewing 19
  revoking 20
  signing files 21
  suspending 19

Public Key Infrastructure User’s Guide 73
D

database records, registration 3, 27
attributes 27
handling by RA 3
DB2 27
Delete Certificate dialog 40
deletion of request, Client application 18
details of certificate 19
device certificate 7, 29
dialog 39
Certificate Renewal 39
Change Password 40
Delete Certificate 40
Export Certificate 41
Import Certificate 41
New Certificate Using a Preregistration File 41
New Certificate Using a Transaction ID 41
Open Certificate 42
Open Smart Card 43
Renew Certificate 43
Revoke Certificate 44
Sign a File 44
Smart Card Properties 45
digital certificate 28
backing up 13
categories 28
database records 27
deleting 18
details 19
expiring 20, 39
exporting to a file 18
for using enrollment services 5, 29
importing from a file 18
managing from Client application 18
managing from enrollment Web page 10
non-renewable 30
recovering 13
renewable 29, 30
requesting from Client application 17
requesting from enrollment Web page 5
summary information 21
types 35
digital signatures 21, 30
Directory access 28
distinguished name 28

enrollment request 3 (continued)
enrollment form 25
evaluating 26
from Client application 17
from enrollment Web page 5
handling by RA 3
life cycle 27
preregistration 25
registration database record 27
registration domain 27
Web browser support 26
enrollment Web page 3, 5
accessing 5
CA certificate for using 29
checking request status 10
enrollment form fields 33
enrollment types 25
request ID 6, 7, 8
scenario for preregistration 25
URL 5
exiting the Client application 23
expiring certificates 20, 39
Export Certificate dialog 41

F
fields, enrollment form 33

H
Help for Client application 45
How do I... topics 5

I
Import Certificate dialog 41
initisc program 15
installing the Client application 14
Internet Explorer browser certificate 6

K
key, compromised 36
key backup, requesting 13
Key Backup Request Web page 13
key recovery 30
key recovery, requesting 13
Key Recovery Request Web page 13
LDAP protocol 28
limits for enrollment 33
list of certificates 21

MD5 With RSA algorithm 44
menus, Smart Card View window 38

Netscape browser certificate 6
New Certificate Using a Preregistration File dialog 41
New Certificate Using a Transaction ID dialog 41
non-renewable certificate 30

Open Certificate dialog 42
Open Smart Card dialog 43
overview 3

Pending request, Client application 18
physical smart cards, enabling 15
PKCS #10 request for certificate 29, 33
PKCS #12 file, backing up 13
PKCS #12 file, recovering 13, 30
PKIX-compliant application 8, 28
preregistration 25
checking request status 10
scenario for tasks 25
using preregistration file 17
using transaction ID 17
preregistration file 10, 17
properties, smart card 22
protocol, Directory access 28
protocols 28
purpose of certificate 35

RA 26
RA Desktop 25, 27
reasons for revocation 36
recovery, key 30
recovery request, issuing key 13
Reference topics 33

registrar 25, 26, 27
registration 26
automated 26
need for 3
policies 27
Web browser support 26
Registration Authority 3, 26
registration database records 3, 27
attributes 27
handling by RA 3
registration domain 27
Renew Certificate dialog 43
renewability 30
renewable certificate 30
renewal
from Client application 19
from enrollment Web page 11
request, deleting in Client application 18
request, enrollment 3
automated evaluation 26
enrollment form 25
evaluating 26
from Client application 17
from enrollment Web page 5
handling by RA 3
life cycle 27
preregistration 25
registration database record 27
registration domain 27
Web browser support 26
request ID 6, 7, 8
revocation
from Client application 20
from enrollment Web page 12
reasons for 36
Revoke Certificate dialog 44

sections, enrollment form 6, 7, 8
secure applications 30
secure resources 3, 30
server certificate 7, 29
SHA1 With RSA algorithm 44
Sign a File dialog 44
signature algorithms 44
signing files 21, 30
smart card 16, 17, 30
changing password 22
enable a physical card 15
exporting certificate from 18
importing certificate to 18
maintenance 22
moving certificate to another 19
opening 22
password 22
physical card 22, 30
properties 22
using a different 18
<table>
<thead>
<tr>
<th>Page</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>16, 17, 30</td>
<td>smart card (continued)</td>
</tr>
<tr>
<td>22</td>
<td>viewing properties</td>
</tr>
<tr>
<td>16, 22, 30</td>
<td>virtual card</td>
</tr>
<tr>
<td>45</td>
<td>Smart Card Properties dialog</td>
</tr>
<tr>
<td>39</td>
<td>Smart Card View window</td>
</tr>
<tr>
<td>21</td>
<td>dialogs</td>
</tr>
<tr>
<td>21</td>
<td>displaying more rows of a table</td>
</tr>
<tr>
<td>45</td>
<td>Help facility</td>
</tr>
<tr>
<td>38</td>
<td>menus</td>
</tr>
<tr>
<td>21</td>
<td>moving between tabs</td>
</tr>
<tr>
<td>21</td>
<td>resizing a column</td>
</tr>
<tr>
<td>39</td>
<td>tables</td>
</tr>
<tr>
<td>21, 39</td>
<td>tabs</td>
</tr>
<tr>
<td>21</td>
<td>summary information, certificates</td>
</tr>
<tr>
<td>19</td>
<td>suspend, putting certificate in from Client application</td>
</tr>
<tr>
<td>11</td>
<td>from enrollment Web page</td>
</tr>
<tr>
<td>37</td>
<td>system requirements</td>
</tr>
<tr>
<td>37</td>
<td>browser enrollment</td>
</tr>
<tr>
<td>37</td>
<td>Client application</td>
</tr>
<tr>
<td>25</td>
<td>Web browser support</td>
</tr>
<tr>
<td>5</td>
<td>Web page, enrolling on accessing</td>
</tr>
<tr>
<td>29</td>
<td>CA certificate for using</td>
</tr>
<tr>
<td>10</td>
<td>checking request status</td>
</tr>
<tr>
<td>33</td>
<td>enrollment form fields</td>
</tr>
<tr>
<td>25</td>
<td>enrollment types</td>
</tr>
<tr>
<td>6, 7, 8</td>
<td>request ID</td>
</tr>
<tr>
<td>25</td>
<td>scenario for preregistration</td>
</tr>
<tr>
<td>5</td>
<td>URL</td>
</tr>
<tr>
<td>29</td>
<td>X.509v3 certificate extensions</td>
</tr>
<tr>
<td>23</td>
<td>uninstalling the Client application</td>
</tr>
<tr>
<td>5</td>
<td>enrollment Web page</td>
</tr>
<tr>
<td>13</td>
<td>key backup request</td>
</tr>
<tr>
<td>13</td>
<td>key recovery request</td>
</tr>
<tr>
<td>20</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>19, 27</td>
<td>registration domain</td>
</tr>
<tr>
<td>35</td>
<td>validity period</td>
</tr>
<tr>
<td>1</td>
<td>Trust Authority, summary</td>
</tr>
<tr>
<td>35</td>
<td>type of certificate</td>
</tr>
<tr>
<td>14</td>
<td>TACInst.exe file</td>
</tr>
<tr>
<td>15</td>
<td>TAClient.ini file</td>
</tr>
<tr>
<td>25</td>
<td>Tell me about... topics</td>
</tr>
<tr>
<td>17</td>
<td>transaction ID</td>
</tr>
<tr>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>29</td>
<td>X.509v3 certificate extensions</td>
</tr>
</tbody>
</table>