Gentran Integration Suite™

Digital Certificates

Version 4.2

Sterling Commerce
An IBM Company

Contents

Introduction to Digital Certificates

Gentran Integration Suite provides a Certificate Wizard to help you manage your digital certificates. Digital certificates are used for secure data transport, EDIINT, and communication between you and your trading partners. The following digital certificates are used in Gentran Integration Suite:

- CA and trusted certificate – a digital certificate for which Gentran Integration Suite does not have the private key. These certificates are stored in standard DER format.
- System certificates – a digital certificate for which the private key is maintained in Gentran Integration Suite. These certificates are stored with the private key in a secure format.

Gentran Integration Suite supports 3 X.509 version of Digital certificates. Digital certificates can be either self-signed or CA-signed. The following is a brief explanation of both terms:

- A *self-signed certificate* is a digital certificate that is signed with the private key that corresponds to the public key in the certificate, demonstrating that the issuer has the private key that corresponds to the public key in the certificate.
- *A CA-signed certificate* is a digital certificate that is signed using keys maintained by certificate authorities. Before issuing a certificate, the CA typically evaluates a certificate requestor to determine that the requestor is in fact the certificate holder referenced in the certificate.

Benefits of Self-signed and CA-signed Digital Certificates

When you and your trading partners are deciding whether to generate a self-signed certificate or purchase a signed certificate from a CA, consider that:

- You can easily create self-signed certificates using Gentran Integration Suite. However, these self-signed certificates are not verified by a trusted third party.
- The primary advantage of using certificates from a CA is that the identity of the certificate holder is verified by a trusted third party. Disadvantages include the extra cost and administrative effort. If you decide to use a third-party certificate, obtain it from a CA.
- A CA provides a centralized source for posting and obtaining information about certificates, including information about revoked certificates.

By default, Gentran Integration Suite trusts all CA certificates and self-signed certificates generated by the application. You can, however, specify whether all or some certificates issued by a specific CA should be trusted. You also can explicitly not trust a self-signed certificate of a trading partner.

Using Digital Certificates

The following is some basic information about how Gentran Integration Suite uses digital certificates:

- Every organization exchanging secure documents must have a certificate. You can use the Certificate Wizard to generate the certificate or it can be generated externally.
- Every trading profile for a trading partner with whom you exchange signed and encrypted documents must have a certificate.
- An organization or trading profile can have only one active certificate at a time. Or, in the case of dual certificates, one active pair of certificates (one for signature, one for encryption).

- An organization or trading profile must have an active certificate to successfully exchange signed and encrypted documents.
- An organization or trading profile can have multiple valid certificates.
- Certificates can be used to sign documents you transmit by all transport methods.
- The key length for a certificate does not have to be the same as that for a trading partner certificate.

Expiration Dates for Certificates

If an adapter and servlet are used for inbound communications (For example: Receiving AS2 data from trading partners), you must monitor the expiration dates of the System certificates to ensure valid certificates are in place. Before the certificates expire, they must be replaced with valid certificates.

Note: A full backup of Gentran Integration Suite should be performed before replacing any certificates. Changes should be performed in a test environment and verified before making changes to the production environment.

About CA Certificates

A *CA certificate* is a digital certificate issued by a certificate authority (CA). The CA verifies trusted certificates for trusted roots. Trusted roots are the foundation upon which chains of trust are built in certificates. In Gentran Integration Suite, trusting a CA root means you trust all certificates issued by that CA. If you elect not to trust a CA root, Gentran Integration Suite does not trust any certificates issued by that CA.

A CA certificate:

- Contains a public key corresponding to the private key, which the CA owns and uses to sign the certificates it issues.
- Is stored separately from trusted certificates. To validate a trusted certificate, you must first check in a CA certificate.

A CA certificate name is not part of the content of the certificate. CA certificates must have meaningful names, according to your file-name conventions, because Gentran Integration Suite identifies them by name in the user interface.

Caution: Although CA certificates are public documents, you must be careful about who has rights to add them. Someone could maliciously add a false CA certificate in order to verify false end-user certificates.

About the Certificate Wizard

The Certificate Wizard is a Gentran Integration Suite Web-deployed application. The Certificate Wizard tool enables you to create:

- *Certificate Signing Requests (CSRs)* – A file is sent by e-mail to a certificate authority to request an X.509 certificate.
- *Key certificates* – A combination of an ASCII-encoded certificate and an ASCII-encoded PKCS12 encrypted private key (key cert.txt).
- Trusted root files – The trusted root file (trusted.txt) contains a list of trusted sources that enable the certificate wizard to validate a key certificate and ensure a secure connection.

Note: Before you can use the certificate wizard, you must download the Java™ Web Start.

Starting the Certificate Wizard

Note: Initial startup may require several minutes, depending on the speed of your connection. You must have downloaded and installed the Java™ Web Start before starting the certificate wizard.

To start the Certificate Wizard:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. In the System Certificates page, next to Run Certificate Wizard, click **Go!**
3. In the Java Web Start display, click **Start**. The Certificate Wizard is displayed.

Starting the Certificate Wizard Offline

Note: Initial startup may require several minutes, depending on the speed of your connection.

To start the Certificate Wizard offline through Java Web Start:

1. From the Windows **Start** menu, select **Programs** > **Java Web Start** > **Java Web Start**.
2. From the **View** menu, select **Downloaded Applications** to view the installed wizard application (or installed instances of the Certificate Wizard).
3. Select the Certificate Wizard application and click **Start**. The Certificate Wizard is displayed.

Generating a Certificate Signing Request (CSR) using the Certificate Wizard

To generate a CSR:

1. Start the Certificate Wizard.
2. In the Certificate Wizard, click the **Certificate Request** tab.
3. Complete the following fields and click **Next**:

Field	Description
Common Name	Name of the client computer. For example, use an e-mail or TCP/IP address. Required.
Country	Your country. Required.
State/Province	Your state or province. Required.
City/Locality	Your city or locality. Required.
Organization/Company Name	Your organization or company name. Required.
Organization Unit	Your unit within your organization or company. For example, a division within a company can represent a unit. Required.

4. To enable the pseudo-random number generator (PRNG) to generate a random number for the public/private key pair, type any random sequence of characters until processing stops.
5. In the Message dialog box that indicates enough random input is now available (random generated number for the public/private key pair), click **OK**, and then click **Next**.
6. Complete the following fields and click **Next**:

Field	Description
Private Key Length	Encryption strength of your private key. Required. Valid values are: ◆ 512 ◆ 768 ◆ 1024 ◆ 2048 **Note:** The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 2048 is the most secure, but also the slowest, and may not work with some applications.
Passphrase	Passphrase to use for encrypting the private key of the certificate. Passphrase must not be more than 20 characters in length. Required.
Confirm Passphrase	Retype the passphrase you indicated for encrypting the private key of the certificate. Required.

7. Complete the following fields and click **Next**:

Field	Description
Key File Name	Either accept the default directory or click **Browse** to select another directory to save the PKCS12-formatted private key (priv.txt is default file name) file. Required.
CSR File Name	Either accept the default directory or click **Browse** to select another directory to save the CSR (csr.txt is default file name) file. Required.

8. In the confirm page, review the information for accuracy and click **Finish** to complete the CSR.

Creating a Key Certificate using Certificate Wizard

To create a key certificate file:

1. Start the Certificate Wizard.
2. In the Certificate Wizard, click the **Generate KeyCert** tab.
3. Either type the directory or click **Browse** to select the directory to which you have saved the private key file (priv.txt).
4. Either type the directory or click **Browse** to select the directory to which you have saved the Digitally-signed (.cer or .crt file) certificate from the CA.
5. Either accept the default directory or click **Browse** to select another directory to save the key certificate (keycert.txt is default file name) file.
6. To create the key certificate, click **Generate**.

Validating the Key Certificate Using the Certificate Wizard

To validate the key certificate:

1. Start the Certificate Wizard.
2. In the Certificate Wizard, click the **Verify Certificate** tab.
3. Complete the following fields:

Field	Description
Passphrase	Passphrase that you indicated for this key certificate when you generated it. Required.
Keycert	Either type or click **Browse** to select the directory to which you have saved the key certificate (keycert.txt file). This field can remain blank if you only want to verify a trusted root certificate file. Optional.
Trusted Root File	Either type or click **Browse** to select the directory to which you have saved the key certificate to obtain the trusted root certificate file (trust.txt.file). Required.

4. Click **Verify** to enable the Certificate Wizard to validate the key certificate. A message displays that includes the verification results for each file you selected.

Creating a Self-Signed Certificate

To create a self-signed certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. Next to Create Self-Signed Certificate, click **Go!**
3. In the **Name** field, type the name of the self-signed certificate. This must be a unique and meaningful name.
4. In the **Organization** field, type the name of the originating organization.
5. In the **Country** field, select the country or origin of the self-signed certificate.
6. In the **E-mail** field, type a contact e-mail address for the person responsible for certificates in the organization, and then click **Next**.
7. In the **Serial Number** field, type the serial number. The serial number is whatever number you want to assign to the self-signed certificate.
8. In the **Duration** field, type the number of days that the self-signed certificate is valid.
9. From the **Key Length** field, select a key length (512, 1024, or 2048).

   Note: The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 2048 is the most secure, but also the slowest, and may not work with some applications.
10. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
    - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
    - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
11. Set the Certificate Signing bit, by selecting the checkbox.
12. In the Confirm page, verify the information about the self-signed certificate, and then click **Finish**.
13. Click **Return** to continue.

Searching for a CA Certificate

To search for a CA certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **CA**.
2. In the CA Digital Certificates, and complete one of the following actions, and then click **Go!**
   - Under Search in the **by Certificate Name** field, type either a portion of the name or the entire name of the CA certificate you are searching for. The CA Digital Certificates page opens, listing all of the CA certificates containing the full or partial name you typed.
   - Under **List in the Alphabetically field**, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting ALL lists all CA certificates. The CA Digital Certificates page opens, listing all of the CA certificates that match your search criteria.

Editing a CA Certificate

To edit a CA certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **CA**.
2. Using either Search or List, locate the CA certificate you want to edit and click **Go!**
3. Next to the CA certificate you want to edit, click **edit**.
4. In the **Certificate Name** field, type a new name for the CA certificate.
5. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. In the Confirm page, verify the information about the CA certificate, and then click **Finish**.
7. Click **Return** to continue.

Checking In a CA Certificate

Note: This procedure assumes that you have already received the CA certificate and it is saved to a file on your local computer.

To check in a CA certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **CA**.
2. Next to Check in New Certificate, click **Go!**
3. In the **Filename** field, type or click **Browse** to select the file name of the CA certificate, and then click **Next**.
4. In the **Certificate Name** field, verify the name of the CA certificate you are checking in.

   Note: For each certificate in the file you selected, the Certificate Name field contains a suggested name built out of the issuer relative distinguished name (RDN) and serial number of the certificate. Following the name is a summary of the identifying information in the certificate. For convenience, Gentran Integration Suite records the name of the certificate in its database. You can change the name to fit your file-naming conventions or to something easier to remember.
5. If you have more than one CA certificate contained in the file you selected, select the check box to the left of each certificate to check in each certificate.
6. Next to Validate When Used, select the validation options, and then click **Next**:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. In the Confirm page, verify the information about the CA certificate you are checking in, and then click **Finish** to check the CA certificate.
8. Click **Return** to continue.

Deleting a CA Certificate

To delete a CA certificate:

1. From **Administration** menu, select **Trading Partner** > **Digital Certificates** > **CA.**
2. In the CA Certificates page, under List, next to Alphabetically, click **Go!**
3. Next to the CA certificate you want to delete, click **delete**.
4. Click **Return** to continue.

Searching for a System Certificate

To search for a system certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. In the system certificates, and complete one of the following actions, and then click **Go!**
   - Under Search in the **by Certificate Name** field, type either a portion of the name or the entire name of the system certificate you are searching for. The System Certificates page opens, listing all of the system certificates containing the full or partial name you typed.
   - Under **List in the Alphabetically field**, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting ALL lists all system certificates. The System Certificates page opens, listing all of the system certificates that match your search criteria.

Identifying a System Certificate

To identify a System certificate:

1. From the **Administration** menu, select **Deployment** > **Services** > **Configuration**.
2. In the List section, select the applicable service or adapter type (For example, B2B HTTP Server Adapter) from the ***by Service Type*** list and click **Go**.
3. From the list of configurations, choose the configuration you are using for your HTTP communication.
4. Click the service name link to see information about the configuration.
5. From the summary information, make a note of certificate type.

Note: If you have multiple configurations, then make a note of each that you are using.

Checking the Expiration Date of a System Certificate

To check the expiration date of a system certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. To view all system certificates select **All** from the Alphabetical drop down list.
3. Click the name of the system certificate you want to view. The Certificate Summary displays.
4. In the Description section of the Certificate Summary, view the Valid Dates field.

Editing a System Certificate

To edit a system certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. Using either Search or List, locate the system certificate you want to edit and click **Go!**
3. Next to the system certificate you want to edit, click **edit**.
4. In the **Certificate Name** field, type a new name for the system certificate.
5. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. In the Confirm page, verify the information about the system certificate, and then click **Finish**.
7. Click **Return** to continue.

Exporting a System Certificate

To export a Gentran Integration Suite system certificate:

Note: This export command is only applicable to Gentran Integration Suite system certificates. You cannot use this command to export system certificates on HSM.

1. Type the following command, with the appropriate parameters:

   `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`

   Note: Use the following parameters with the ExportSystemCert.sh command:

Parameter	Description
keyname	The keyname of the Gentran Integration Suite system key to export.
pkcs12filename	The name of the file where exported information is written.
pkcs12storepass	Store password that protects the store.
pkcs12keypass	Key password that protects the key.

Deleting a System Certificate

To delete a system certificate:

Note: You may want to export a copy of the system certificate to your local disk before you delete it. This will provide you with a backup copy of the certificate. The OpsDrv, OpsKey, or UIKeys are system certificates that can not be deleted.

Note: HSM System certificates are not exported using the same export command as other certificates. See HSM for more information.

1. From **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System.**
2. In the System Certificates page, under List, next to Alphabetically, click **Go!**
3. Next to the system certificate you want to delete, click **delete**.
4. A warning message is displayed “Do you want to permanently delete this system certificate? (Can not be undone), click **OK.**
5. Review the information on the system certificate delete page, click **delete**.
6. Click **Return** to continue.

Checking Out a System Certificate

Note: To export a system certificate, you must check out the certificate. The following procedure exports only the public certificate, not the private key, and provides you with a public certificate to send to a trading partner.

To check out a system certificate:

1. From **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. Using either Search or List, locate the system certificate you want to check out.
3. Next to the system certificate you want to check out, click **check out**.
4. In the **Check Out System Certificate** dialog box, select one of the following formats for the certificate, and then click **Go!**:
   - BASE64 – This option uses BASE64 encoding on the standard DER certificate.
   - DER – This standard format for digital certificates is accepted by most applications.
5. In the **File Download** dialog box, click **Save**.
6. In the **Save As** dialog box, select the location where you want to save the certificate, and then click **Save**.

   Note: The option to open the certificate is not supported. You must open the certificate within the Windows operating system. If you receive the error message, “This is an invalid Security Certificate file,” open the file in a text editor and delete any blank lines before -----BEGIN CERTIFICATE-----. Save the edited file and Windows should open the file.
7. In the **Check Out System Certificate** dialog box, click **Close**. You are now back to the System Certificate page.
8. Click **Return** to continue.

Searching for a Trusted Certificate

To search for a trusted certificate:

1. From the Administration menu, select **Trading Partner** > **Digital Certificate** > **Trusted**.
2. In the Trusted Digital Certificates page, complete one of the following actions, and then click **Go!**:
   - Under Search in the **by Certificate Name** field, type either a portion of the name or the entire name of the trusted certificate you are searching for. The Trusted Digital Certificates page opens, listing all of the trusted certificates containing the full or partial name you typed.
   - Under **List in the Alphabetically field**, select **ALL** or the letter that begins the name of the trusted certificate you are searching for. Selecting ALL lists all of the trusted certificates. The Trusted Digital Certificates page opens, listing all of the trusted certificates that match your search criteria.

Editing a Trusted Certificate

To edit a trusted certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **Trusted**.
2. Using either Search or List, locate the trusted certificate you want to edit and click **Go!**
3. Click **edit** next to the trusted certificate for which you want to edit.
4. In the **Certificate Name** field, type a new name for the trusted certificate.
5. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. In the Confirm page, verify the information about the trusted certificate, and then click **Finish**.
7. Click **Return** to continue.

Checking In a Trusted System Certificate

Note: This procedure assumes that you have already saved the trusted system certificate to a file on your local computer.

To check in a trusted system certificate:

1.From the **Administration** menu, select **Trading Partner** > **Digital Certificate** > **Trusted**.

2. Next to Check in New Certificate, click **Go!**
3. In the **Filename** field, type or click **Browse** to select the file name of the trusted certificate, and then click **Next**.
4. In the **Certificate Name** field, verify the name of the trusted certificate you are checking in.

   Note: For each certificate in the file you selected, the Certificate Name field contains a suggested name built out of the issuer relative distinguished name (RDN) and serial number of the certificate. Following the name is a summary of the identifying information in the certificate. For convenience, Gentran Integration Suite records the name of the certificate in its database. You can change the name to fit your file-naming conventions or to something easier to remember.
5. If you have more than one trusted certificate contained in the file you selected, select the check box to the left of each certificate to check in each certificate.
6. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. In the Confirm page, verify the information about the trusted certificate you are checking in, and then click **Finish** to check the trusted certificate in.
8. Click **Return** to continue.

Deleting a Trusted System Certificate

To delete a trusted system certificate:

1. From **Administration** menu, select **Trading Partner** > **Digital Certificates** > **Trusted.**
2. In the Trusted Certificates page, under List, next to Alphabetically, click **Go!**
3. Next to the trusted certificate you want to delete, click **delete**.
4. Click **Return** to continue.

Importing a PKCS12 System Certificate

To import a PKCS12 system certificate:

1. Type the following command, with the appropriate parameters:

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
   pkcs12storepass pkcs12keypass keystoretype keystoreprovider
   storepass keypass
   ```

   Note: Use the following parameters with the ImportSystemCert.sh command:

Parameter	Description
systempass	The system passphrase.
certname	The name to assign to the system certificate in the database.
pkcs12file	The name of the PKCS12 file to import.
pkcs12storepass	The store passphrase used for the generation of the PKCS12 file.
pkcs12keypass	A valid passphrase for the PKCS12 file.
keystoretype	The keystore type to import. Valid value = CRYPTOKI.
keystoreprovider	The provider type. Eracom is the only HSM supported provider type. **Note:** ERACOM or ERACOM.n if you are importing certificates to a slot other than the first position
storepass	The PIN for the slot on the Eracom device where the keystore resides.
keypass	The PIN for the slot on the Eracom device.

Checking In a PKCS12 System Certificate

Note: This procedure assumes that you have already saved the PKCS12 system certificate to a file on your local computer.

To check in a PKCS12 system certificate:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. In the System Certificates page, under Check in, next to PKCS12 Certificate, click **Go!**
3. In the PKCS12 certificates page, complete the following actions:
   a. In the **Certificate Name** field, type a unique and meaningful name for the PKCS12 certificate.
   b. In the **Private Key Password** field, type the private key password. This is the password used to encrypt the PKCS12 certificate.
   c. In the **Key Store Password** field, type the key store password. This is the password for the PKCS12 object. It may be the same as the private key password.
   d. In the **Filename** field, type or click **Browse** to select the file name of the PKCS12 certificate, and then click **Next**.
4. Next to Validate When Used, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
5. In the Confirm page, verify the information about the PKCS12 certificate, and then click **Finish**.
6. Click **Return** to continue.

Importing a Pem System Certificate

To import a pem system certificate:

Note: Gentran Integration Suite only supports pem keys encrypted with DES or 3DES.

1. Type the following command with the appropriate parameters:

   ```
   ./ImportSystemCert.sh -pem systempass certname file password keystoretype
   keystoreprovider storepass keypass
   ```

   Note: Use the following parameters with the ImportSystemCert.sh command:

Parameter	Description
systempass	The system passphrase.
certname	The name to assign to the system certificate in the database.
file	The name of the File to import.
password	The store passphrase for the pem file.
keystoretype	The keystore type to import. Valid value = CRYPTOKI.
keystoreprovider	The provider type. Eracom is the only HSM supported provider type. **Note:** ERACOM or ERACOM.n if you are importing certificates to a slot other than the first position
storepass	The PIN for the slot on the Eracom device where the keystore resides.
keypass	The PIN for the slot on the Eracom device

Importing a Key System Certificate

To import a key system certificate:

1. Type the following command, with the appropriate parameters:

   ```
   ./ImportSystemCert.sh -keycert systempass certname file password
   keystoretype keystoreprovider storepass keypass
   ```

   Note: Use the following parameters with the ImportSystemCert.sh command:

Parameter	Description
systempass	The system passphrase.
certname	The name to assign to the system certificate in the database.
file	The name of the File to import.
password	The store passphrase for key certificate file.
keystoretype	The keystore type to import. Valid value = CRYPTOKI.
keystoreprovider	The provider type. Eracom is the only HSM supported provider type. **Note:** ERACOM or ERACOM.n if you are importing certificates to a slot other than the first position
storepass	The PIN for the slot on the Eracom device where the keystore resides.
keypass	The PIN for the slot on the Eracom device.

Checking In a Key System Certificate

Note: This procedure assumes that you have already saved the key system certificate to a file on your local computer.

To check in a key system certificate:

1. From Administration menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. In the System Certificates page, under Check in, next to Key Certificate, click **Go!**
3. In the **Certificate Name** field, type the key certificate name. This should be a unique and meaningful name.
4. In the **Private Key Password** field, type the private key password. This is the password used to encrypt the private key.
5. In the **Filename** field, type or click **Browse** to select the file name of the key certificate, and then click **Next**.
6. Next to **Validate When Used**, select the validation options, and then click **Next**. Validation options include:
   - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
   - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. In the Confirm page, verify the information about the key certificate you are checking in, and then click **Finish** to check the key certificate in.
8. Click **Return** to continue.

Importing a Keystore System Certificate

To generate a Gentran Integration Suite keystore system certificate on HSM:

1. Type the following command, with the appropriate parameters:

   ```
   ./ImportSystemCert.sh -keystore systempass certname alias keystoretype
   keystoreprovider storepass keypass
   ```

   Note: Use the following parameters with the ImportSystemCert.sh command:

Parameter	Description
systempass	The system passphrase.
certname	The name to assign to the system certificate in the database.
alias	The key name stored in the HSM. Only alias names containing characters a-z, A-Z, 0-9 or hyphen (-), and whose total length is no longer than the system GUID length.
keystoretype	The keystore type to import. Valid value = CRYPTOKI.
keystoreprovider	The provider type. Eracom is the only HSM supported provider type. **Note:** ERACOM or ERACOM.n if you are importing certificates to a slot other than the first position
storepass	The PIN for the slot on the Eracom device where the keystore resides.
keypass	The PIN for the slot on the Eracom device

Downloading Java Web Start

To download Java Web Start:

1. From the **Administration** menu, select **Trading Partner** > **Digital Certificates** > **System**.
2. In the System Certificates page, next to Java Web Start, click **Download**.
3. In the **File Download** dialog box, select the **Save** option and click **OK**.
4. In the **Save as** dialog box, select a directory on your client computer and click **Save** to begin downloading Java Web Start.

   Note: The download may require several minutes, depending on the speed of your connection.
5. When the download is complete, close the **Download** dialog box if it remains open.
6. Open the directory where you downloaded the file for Java Web Start.
7. Double-click the file **javaws-1_0_1_02-win-int-rt.exe** to begin the installation process.
8. After reading the license agreement, click **Accept**.
9. In the **Installation Directory** dialog box, either accept the default directory or click **Browse** to select another directory to install Java Web Start, and then click **Next**.
10. When you receive a message that setup was unable to detect a usable Java 2 Runtime Environment, either accept the default installation directory or click **Browse** to select another installation directory, and then click **OK**.

    The **Installing Files** dialog box opens and displays the in-progress installation. When the installation is complete, the setup program prompts you to read the Readme file. You can now access the Certificate Wizard.

Exiting the Certificate Wizard

To exit the Certificate Wizard:

1. On the Certificate Wizard, click **Exit**.
2. On the Exit Warning box, click **Yes** to verify you want to exit.

Removing the Certificate Wizard

To remove an instance of the Certificate Wizard from the Java Web Start Manager:

1. On the computer where the wizard is installed, from the Windows **Start** menu, select **Programs** > **Java Web Start** > **Java Web Start**.
2. From the **View** menu, select **Downloaded Applications** to view the wizard application (or installed instances of the wizard).
3. Select the Certificate Wizard (or the instance of the wizard) that you want to remove from the application window.
4. From the **Application** menu, select **Remove Applications**.

Index