The InterSystems Public Key Infrastructure

Version 2023.1
2024-07-11

InterSystems Corporation   1 Memorial Drive   Cambridge MA 02142   www.intersystems.com

The InterSystems Public Key Infrastructure
InterSystems IRIS Data Platform Version 2023.1 2024-07-11

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

The InterSystems Public Key Infrastructure **1**

- 1 About the InterSystems Public Key Infrastructure (PKI) 1
  - 1.1 Help for Management Portal PKI Tasks 2
- 2 Certificate Authority Server Tasks 2
  - 2.1 Configure an InterSystems IRIS Instance as a Certificate Authority Server 2
  - 2.2 Manage Pending Certificate Signing Requests 6
- 3 Certificate Authority Client Tasks 8
  - 3.1 Configure an InterSystems IRIS Instance as a Certificate Authority Client 8
  - 3.2 Submit a Certificate Signing Request to a Certificate Authority Server 9
  - 3.3 Get Certificate(s) from Certificate Authority Server 10

The InterSystems Public Key Infrastructure

Important: The InterSystems PKI is for testing purposes only. Do *not* use it in a production setting.

This document covers the following topics:

- About the InterSystems Public Key Infrastructure (PKI)
- Certificate Authority Server Tasks
  - Configuring an InterSystems IRIS® Instance as a Certificate Authority Server
  - Managing Pending Certificate Signing Requests
- Certificate Authority Client Tasks
  - Configuring an InterSystems IRIS Instance as a Certificate Authority Client
  - Submitting a Certificate Signing Request to a Certificate Authority Server
  - Getting Certificate(s) from the Certificate Authority Server

1 About the InterSystems Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) provides a means of creating and managing private keys, public keys, and certificates. These are used for cryptographic operations including encryption, decryption, and digital signing and signature verification. Certificates provide a means of associating a public key with an identity. To do this, a PKI includes a trusted third party known as a certificate authority (CA).

The InterSystems PKI implementation gives InterSystems IRIS the ability to serve as a Certificate Authority (CA). An instance of InterSystems IRIS acting as a CA is known as a CA server; an instance of InterSystems IRIS using a CA's services is known as a CA client. A single instance of InterSystems IRIS can be both a CA server and a CA client. As a CA server, an instance can either generate and use a self-signed CA Certificate, or it can use a CA Certificate issued by a commercial third party or product. As a CA client, an instance is associated with a CA server; the CA client's certificate is available for use with TLS, XML encryption, and signature verification; there is also the option of configuring a CA client to serve as an intermediate CA. Communications involving the PKI occur through web services.

When establishing itself as a CA server, an instance of InterSystems IRIS either creates a public/private key pair and then embeds the public key in a self-signed X.509 certificate or it uses a private key and X.509 certificate signed by an outside CA. X.509 is an industry-standard certificate structure that associates a public key with both identifying information for an entity and other related data; this identifying information is known as a subject Distinguished Name (DN), and consists of various specific information regarding an entity's organization, location, or both. You can use X.509 certificates to provide a high level of public-key–based security if, and only if, appropriate security policies regarding the protection of private keys and the issuance of certificates are enforced, including strict control of the CA server's private key file, preferably stored on removable media which can be physically secured when not in use.

To use the InterSystems IRIS PKI infrastructure from the Management Portal, all actions start from the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).

For more background on PKI and CAs, see the appendix, "About Public Key Infrastructure (PKI)." For technical details about the TLS calls underlying the InterSystems PKI, see the OpenSSL library. For technical details about X.509 certificates, see RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile."

1.1 Help for Management Portal PKI Tasks

The following are links to help for PKI tasks:

- Certificate Authority Client
  - Submit Certificate Signing Request to Certificate Authority server
  - Get Certificate(s) from Certificate Authority server
  - Configure local Certificate Authority client
- Certificate Authority Server
  - Process pending Certificate Signing Requests
  - Configure local Certificate Authority server

2 Certificate Authority Server Tasks

An InterSystems IRIS instance can serve as a certificate authority (CA) server. This involves:

1. Configuring an InterSystems IRIS instance as a CA server. This involves providing information that is either related to the certificate or that the CA server uses for processing certificate signing requests.
2. Managing pending certificate signing requests (CSRs). This is the ongoing work of a CA server.

Note: Because these tasks are for the CA server administrator, this section is addressed to those administrators. This differs from the tasks in the CA client tasks, which are addressed to CA client administrators/technical contacts.

2.1 Configure an InterSystems IRIS Instance as a Certificate Authority Server

Before any PKI operations are possible, you need to configure an InterSystems IRIS instance as a Certificate Authority (CA) server. This involves either:

- Configuring a CA Server with a New Private Key and Certificate
- Configuring a CA Server with an Existing Private Key and Certificate

It may also involve reinitializing a CA server.

2.1.1 Configure a CA Server with a New Private Key and Certificate

If you are creating a new private key and certificate, the procedure is:

1. For the selected InterSystems IRIS instance, in the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Server**, select **Configure Local Certificate Authority server**. This displays fields for (1) the file name root for the CA server's certificate and private key and (2) the directory that holds these files.

Important: If you specify a path and file name root that point to an existing certificate and private key, InterSystems IRIS uses these for the CA server. Otherwise, it creates a new certificate and private key. (Also, if only one of the files exists, InterSystems IRIS renames it by appending the `.old` suffix to it and creates new files.)

The fields are:

- **File name root for Certificate Authority's Certificate and Private Key files (without extension)** — Required. Specifies the part of the name of the private key and certificate files that is common to each. This can be for an existing pair of files or for a new pair of files. Hence, if you select `MyCA` as the file name root, the private key is stored in the MyCA.key file and the certificate is stored in the MyCA.cer file. Valid characters for this field are alphanumeric characters, the hyphen, and the underscore. The root cannot be the string "cache".
- **Directory for Certificate Authority's Certificate and Private Key files** — Required. The path to a directory for storing the CA's certificate and private key files; if the directory does not exist, InterSystems IRIS attempts to create it. This directory should always be on an external device (not a local hard drive or a network server), preferably on an encrypted external device. As this is the directory that holds the CA's private key, it is extremely important that this be a completely secure location. If you provide a relative path here, the path is relative to <install-dir>/mgr/ for the InterSystems IRIS instance.

3. Click **Next** to continue.
4. The fields that appear next depend on whether you are creating a new private key and certificate pair or using an existing private key and certificate. When you are creating a new private key and certificate, InterSystems IRIS displays the following fields:

   - **Password to Certificate Authority's Private Key file** and **Confirm Password** — Required. The password to encrypt and decrypt the CA's private key file.
   - **Certificate Authority Subject Distinguished Name** — The set of one or more name-value pairs that define the distinguished name (DN) that describes the bearer of the CA certificate. You must provide a value for at least one attribute. The attributes are:
     - **Country** — A two-letter code identifying the country, using the ISO country codes.
     - **State or Province** — The name of the CA's state or province. The convention is not to use this field for CA certificates.
     - **Locality** — The name of the CA's municipality. The convention is not to use this field for CA certificates.
     - **Organization** — Name of the organization that is administering the CA. By convention, this value is spelled out in full, such as "InterSystems Corporation," rather than simply "InterSystems" or "InterSystems Corp."
     - **Organizational Unit** — Any other organizational information or special commentary on the CA. Examples of this can include the CA's department, a statement that the CA is for use only within an enterprise, and so on.
     - **Common Name** — A descriptive name for the CA, such as "Documentation Test CA."
   - **Validity period for Certificate Authority's Certificate (days)** — Required. The validity period (lifespan) for the CA certificate itself.
   - **Validity period for Certificates issued by Certificate Authority (days)** — Required. The validity period (lifespan) for certificates that the CA issues for its clients.
   - **Configure email** — Information required for the email account for managing the CA and its tasks.
     - **SMTP server** — The Simple Mail Transfer Protocol (SMTP) server that handles the CA mail in the form of a fully qualified host name, such as "MyMachine.MyDomain.com".

  - **SMTP username** — A username that can be authenticated by the specified SMTP server. This field does not require a fully qualified username.
  - **SMTP password** — The password associated with the SMTP username.
  - **Confirm password** — A confirmation of the password associated with the SMTP username.
  - **Certificate Authority server administrator's email address** — The user who receives certificate signing requests for the CA. This field requires a fully qualified username, such as “CAMgr@MyDomain.com”.

5. Complete these fields as required and click **Save**. InterSystems IRIS displays a message indicating success, such as:

   ```
   Certificate Authority server successfully configured.
   Created new files: C:\pki\FileNameRoot.cer .key, and .srl.
   Certificate Authority Certificate SHA-1 fingerprint:
   E3:FB:30:09:53:90:9A:31:30:D3:F0:07:8F:64:65:CD:11:0A:1A:A2
   Confirmation email sent to: CAserver-admin@intersystems.com
   ```

   This indicates that a private key, certificate, and their associated SRL (serial) file have been created. (Otherwise, InterSystems IRIS displays an error message.)

   Once the files have been created, it is *strongly* recommended that you store the private key on removable media that can be physically secured.

   WARNING! It is critical that you properly protect all private keys, and most important that you protect the private key of a CA. The exposure of a private key can result in security breaches, data exposure, financial losses, and legal vulnerability.

   If it has succeeded, InterSystems IRIS has performed the following actions:

   - Creating a key pair.
   - Saving the private key to a file to a specified location with a specified file name root (see below).
   - Creating a self-signed CA certificate containing the public key.
   - Saving the certificate to a file to a specified location with a specified file name root (see below).
   - Creating a counter of the number of certificates issued and storing it in an SRL (serial) file in the same directory as the certificate and the private key. (Each time the CA issues a new certificate, InterSystems IRIS gives the certificate a unique serial number based on this counter and then increments the value in the SRL file.)

Once you have created the CA private key and certificate, you can process certificate signing requests (CSRs). When a CA client creates a CSR, you, as CA administrator, will receive email notification about this.

2.1.2 Configure a CA Server with an Existing Private Key and Certificate

If you are using an existing private key and certificate (such as from another InterSystems IRIS CA, or from an external CA, such as a commercial CA), the procedure is:

1. Create or obtain a private key and certificate. The certificate must be in PEM format, or you must be able to convert it to PEM format.
2. If they do not already have identical file name roots, rename them as *filenameroot*`.cer` for the certificate and *filenameroot*`.key` for the private key, where *filenameroot* is the file name root you wish to use.
3. Store both files in the same directory, making sure that this directory is accessible to the InterSystems IRIS instance that you are configuring as a CA server. This directory should always be on an external device (not a local hard drive

or a network server), preferably on an encrypted external device. As this is the directory that holds the CA’s private key, it is extremely important that this be a completely secure location.

WARNING! It is critical that you properly protect all private keys, and most important that you protect the private key of a CA. The exposure of a private key can result in security breaches, data exposure, financial losses, and legal vulnerability.

4. For the selected InterSystems IRIS instance, in the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
5. On the **Public Key Infrastructure** page, under **Certificate Authority Server**, select **Configure Local Certificate Authority server**. Complete the fields on this page as follows:
    - **File name root for Certificate Authority’s Certificate and Private Key files (without extension)** — Required. The part of the name of the private key and certificate files that is common to each. For this value, use the file name root that the files have or that you selected in step 2 of this procedure.
    - **Directory for Certificate Authority’s Certificate and Private Key files** — Required. The path to a directory that holds the CA’s certificate and private key files. For this value, use the directory that you selected in step 3. If you provide a relative path here, the path is relative to <install-dir>/mgr/ for the InterSystems IRIS instance.
6. Click **Next** to continue.
7. The fields that appear next depend on whether you are creating a new private key and certificate pair or using an existing private key and certificate. When you are using an existing private key and certificate, InterSystems IRIS displays the following fields:
    - **Validity period for Certificates issued by Certificate Authority (days)** — Required. The validity period (lifespan) for certificates that the CA issues for its clients.
    - **Configure email** — Information required for the email account for managing the CA and its tasks.
        - **SMTP server** — The Simple Mail Transfer Protocol (SMTP) server that handles the CA mail in the form of a fully qualified host name, such as “MyMachine.MyDomain.com”.
        - **SMTP username** — A username that can be authenticated by the specified SMTP server. This field does not require a fully qualified username.
        - **SMTP password** — The password associated with the SMTP username.
        - **Confirm password** — A confirmation of the password associated with the SMTP username.
        - **Certificate Authority server administrator's email address** — The user who receives certificate signing requests for the CA. This field requires a fully qualified username, such as “CAMgr@MyDomain.com”.

    Important: If the Management Portal displays more fields than these, then you have not properly directed it to the private key and certificate that you wish to use. If you complete all the displayed fields, click **Save**, and there is success, InterSystems IRIS will have created a new private key and certificate for the CA server.
8. Click **Save**. When you save the configuration information for the local CA server, InterSystems IRIS uses the existing certificate and private key. (It will also create an SRL file, if one does not exist.) It will display a success message such as:

```
Certificate Authority server successfully configured.
Using existing files: C:\pki\FileNameRoot.cer and .key
Certificate Authority Certificate SHA-1 fingerprint:
E3:FB:30:09:53:90:9A:31:30:D3:F0:07:8F:64:65:CD:11:0A:1A:A2
Confirmation email sent to: CAserver-admin@intersystems.com
```

As with creating a new private key and certificate, at this point, the CA server is configured and is now ready to process certificate signing requests (CSRs). Again, when a CA client creates a CSR, you, as CA administrator, will receive email notification about this.

2.1.3 Reinitialize a CA Server

If you have already configured an instance as a CA server, then there is a **Reinitialize** button on the page for configuring a CA. Selecting it has the following effects:

- It deletes all configuration information for the CA server.
- It discards all information for issued certificates.
- It discards all certificate signing requests pending with the CA.

Note: Reinitialization does not delete the files containing the private key or existing certificate for the CA, nor does it delete the CA's existing SRL file; in fact, these are still valid and can be used. Also, it does not render any already signed certificates invalid.

When you click the button, there is a prompt to confirm that you want to reinitialize the CA. After reinitialization, you can configure a new CA server.

2.2 Manage Pending Certificate Signing Requests

Once the Certificate Authority (CA) server has been configured, the principal task associated with the CA server is managing certificate signing requests (CSRs) from potential CA clients. This can involve:

- Processing a Certificate Signing Request (CSR)
- Deleting a Certificate Signing Request (CSR)

If processing leads to approving the request, the CA server issues an X.509 certificate signed with the CA's private key, and sends email notification of the issued certificate's serial number to the CA client's technical contact. It is also possible to delete (that is, reject) a request.

A critical step in this process is *verification*, in which the CA administrator uses communications that prevent impersonation to verify the identity of the requester, the authority of the technical contact to hold a certificate with the requested DN, and the purpose for which the certificate is being issued. (To do this, the CA server's administrator uses the contact information received from the potential CA client along with the CSR.)

2.2.1 Process a Certificate Signing Request (CSR)

To process a request is to convert the CSR into a certificate. The procedure is:

1. In the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Server**, select **Process pending Certificate Signing Requests**. This displays a table of CSRs that the CA has received and not processed or deleted; to the right of each CSR there are **Process** and **Delete** links.
3. Mount the media containing the CA server certificate and private key files. (This is the media on which you stored these files while configuring an InterSystems IRIS instance as a CA server.)
4. To process a CSR, click **Process**. This displays the contents of the CSR.
5. Prior to issuing the certificate, you need to specify the use of the certificate. The choices for the **Certificate Usage** radio buttons specify which operations the certificate can perform:

- **TLS/SSL and XML security** — For CA clients that are directly using various security capabilities within InterSystems IRIS.
- **Intermediate Certificate Authority** — For CA clients that will themselves be serving as CAs for other instances of InterSystems IRIS.
- **Code signing** — For CA clients that perform code signing.

6. **Important:** This step requires that you verify the identity of the technical contact for the potential CA client using a means that prevents impersonation.

   As the instructions on this page specify, you must contact the designated technical contact for the instance that has submitted the CSR. According to the policies of your organization, contact this person by phone or in person and verify:

   - This person's identity
   - This person's authority to hold a certificate containing the Subject Distinguished Name shown above, signed by the CA for which you are responsible
   - That the SHA-1 fingerprint shown above matches the one reported to them when they submitted the certificate signing request

7. Once you have specified the purpose of the certificate and verified the relevant information with the technical contact, you can issue the certificate. To do this, click **Issue Certificate**. This causes the page to display the **Password for Certificate Authority's Private Key file** field.
8. In the **Password for Certificate Authority's Private Key file** field, enter the password to decrypt the CA server's private key file. If you created the private key and certificate with InterSystems IRIS, this is the value you entered in the **Password to Certificate Authority's Private Key file** field; if you created the private key and certificate using other tools, it is the password, if any, that you provided to those tools for this purpose.
9. Click **Finish** to create the certificate. If successful, InterSystems IRIS displays a message such as

   ```
   Certificate number 31 issued for Certificate Signing Request
   "Santiago Development Group"
   ```

10. Remove the media holding the CA server's certificate and private key, and store it in a secure location.

InterSystems IRIS has now created the certificate and notified the technical contact for the CA client by email that the certificate is available for download. The CA client's technical contact can now download the certificate to the client host.

2.2.2 Delete a Certificate Signing Request (CSR)

To delete a request, the procedure is:

1. In the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Server**, select **Process pending Certificate Signing Requests**. This displays a table of CSRs that the CA has received and not processed or deleted; to the right of each CSR there are **Process** and **Delete** links.
3. To delete a CSR, click **Delete**. This displays a confirmation dialog.
4. In the confirmation dialog, click **OK**.
5. Complete these fields as required and click **Save**.

This deletes the CSR.

3 Certificate Authority Client Tasks

A certificate authority (CA) client has one-time setup tasks, which are:

1. Configuring the InterSystems IRIS instance as a CA client. This involves providing location about the CA server to the potential CA client; it also includes providing contact information about the CA client's technical contact.
2. Getting a copy of the CA certificate. This allows for verifying other certificates.

After setup tasks, the CA client tasks are:

1. Submitting a certificate signing request (CSR) to the CA server. From the user's perspective, this involves specifying a distinguished name (DN) and other information. (This may happen repeatedly, if the instance has reason to have multiple distinct certificates.)
2. Getting copies of various certificates. In addition to the CA client's own certificate, this includes any other certificates that the CA server has issued.

After performing these tasks, the CA client can then perform the operations that require use of the PKI. These are tasks in which it is known as an *end entity*, since it is at the end of a secured connection.

Note: Because these tasks are for the CA client administrators/technical contacts, this section is addressed to those individuals. This differs from the tasks in the Certificate Authority Server Tasks, which are addressed to CA server administrators.

3.1 Configure an InterSystems IRIS Instance as a Certificate Authority Client

The procedure to configure an InterSystems IRIS instance as a certificate authority (CA) client involves providing location about the CA server to the potential CA client; it also includes providing contact information about the CA client's technical contact. The steps are:

1. In the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Client**, select **Configure Local Certificate Authority Client**. The fields on this page are:
   - **Certificate Authority server hostname** — Required. The fully qualified name of the machine of the CA server. (Specifically, this is a machine on which an instance of InterSystems IRIS is running, and this instance is serving as a CA server. It must be configured as a CA server prior to configuring any instance as a CA client.)
   - **Certificate Authority WebServer port number** — Required. The webserver port number for the instance of InterSystems IRIS serving as the CA server.
   - **Certificate Authority server path** — Required. The path of the web service of the CA server. By default, this is /isc/pki/PKI.CAServer.cls. (This value is used along with the server hostname and port number to contact the web service for the CA.)
   - **Local technical contact** — The person who provides verification information to the CA server on behalf of the CA client. For this person, the following information is required:
     - **Name** — Required. The name of the technical contact for the CA client.
     - **Phone number** — The contact's phone number. This is so that the CA administrator can contact the CA client's technical contact to perform verification prior it issuing the CA client's certificate. The phone number is not required, since InterSystems IRIS does not require a particular mechanism of verification; for example, it could happen in person.

  - **Email address** — The contact’s email address. This is so that the CA client’s technical contact can receive email notification that the CA server has processed the client’s CSR and issued a certificate. The email address is not required, since the server administrator can use some other means to contact the client’s technical contact about the newly issued certificate.

3. Complete these fields as required and click **Save**.

InterSystems IRIS acknowledges success through a message such as “Certificate Authority client successfully configured.” At this point, the next task is to download the CA server’s certificate.

3.2 Submit a Certificate Signing Request to a Certificate Authority Server

Once an instance of InterSystems IRIS is configured as a certificate authority (CA) client, you can then submit a certificate signing request (CSR) to the CA server. On the surface, this involves specifying a distinguished name (DN) and other information. Under the covers, the CA client performs several actions:

1. Generating a public/private key pair.
2. Creating a Certificate Signing Request (CSR) containing the public key and a specified DN.
3. Submitting that to the CA server using a web service.

The PKI infrastructure automatically provides the CSR to the CA server, acknowledges the submission, and sends email notification to the CA server’s administrator. The submission includes your contact information as the local technical contact for the CA client. The CA administrator then processes the CSR by using communications that prevent impersonation to verify the identity of the requester, the authority of the technical contact to hold a certificate with the requested DN, and the purpose for which the certificate is being issued. If the request is approved, the completion of the process includes the CA server creating a certificate.

To submit a CSR to a CA server, the procedure is:

1. In the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Client**, select **Submit Certificate Signing Request to Certificate Authority Server**. The fields on this page are:
   - **File name root for local Certificate and Private Key files (without extension)** — Required. Specifies the part of the name of the private key and certificate files that is common to each. Hence, if you select `CAClient` as the file name root, the private key is stored in the CAClient.key file and the certificate is stored in the CAClient.cer file. Valid characters for this field are alphanumeric characters, the hyphen, and the underscore. The root cannot be the string “cache”.
   - **Password to Certificate Authority's Private Key file** and **Confirm Password** — Optional. The password that for encrypting and decrypting the CA client’s private key.
   - **Subject Distinguished Name** — The set of one or more name-value pairs that define the distinguished name (DN) that describes the bearer of the client certificate. You must provide a value for at least one attribute. The attributes are:
     - **Country** — A two-letter country code for the country, using the ISO country codes.
     - **State or Province** — The name of the state or province, spelled out in full.
     - **Locality** — The name of the municipality, spelled out in full.
     - **Organization** — Name of the organization with which the certificate is associated. By convention, this value is , spelled out in full, such as “InterSystems Corporation,” rather than simply “InterSystems” or “InterSystems Corp.”

   - **Organizational Unit** — Any other organizational information, such as a department.
   - **Common Name** — A descriptive name for the client, such as "Documentation Test Client."

3. Complete these fields as required and click **Save**. If successful, InterSystems IRIS then displays a message such as:

   ```
   SHA-1 Fingerprint:
   0C:DA:5F:06:04:C7:AE:64:61:9C:5C:29:35:49:88:0D:B6:E5:7D:98,
   Certificate Signing Request "CAClient060412"
   successfully submitted to the Certificate Authority at instance MyCA
   on node CATESTCLIENT.CATESTDOMAIN.COM
   ```

   If InterSystems IRIS has successfully created a CSR, it has performed the following actions:

   - Creating a key pair.
   - Saving the private key to a file in the manager's directory with the specified file name root.
   - Creating a CSR that includes the public key and saving it to a file in the manager's directory with the specified file name root.
   - Submitting that CSR to the CA using the host name, port, and path specified as part of the CA client configuration process.

   (If the process does not succeed, InterSystems IRIS displays an error message.)

   Once the files have been created, it is strongly recommended that you store this sensitive information on encrypted, removable media that can be physically secured.

4. Make a copy of the SHA-1 fingerprint that InterSystems IRIS displays.

   Important: Do not lose this information, as you will need to provide this later, as part of the verification process.

5. At this point, you have used InterSystems IRIS to create and submit the CSR. When the administrator of the CA contacts you, provide the SHA-1 fingerprint that you copied in the last step. The administrator will then create certificate for you, which you can obtain as described in Get Certificate(s) from Certificate Authority Server.

3.3 Get Certificate(s) from Certificate Authority Server

Once a certificate authority (CA) client has been configured, it can then download any certificate associated with the CA server. This includes:

- The CA server certificate.
- Its own certificate. This is available if the CA client has submitted a certificate signing request (CSR) to the CA server and the CA server has approved the request.
- Any other certificates that the CA server has created for any other CA clients.

The procedure to obtain certificates is:

1. In the Management Portal, go to the **Public Key Infrastructure** page (**System Administration** > **Security** > **Public Key Infrastructure**).
2. On the **Public Key Infrastructure** page, under **Certificate Authority Client**, select **Get Certificate(s) from Certificate Authority server**. This displays a list of available certificates to download, as well as a button that displays certificates issued for the current instance (whether downloaded or not). Ordinarily, you need both the CA server certificate as well as your own. There are several tasks you can perform from this page:

   - To download the CA certificate, click **Get Certificate Authority Certificate**. A confirmation message such as

```
Certificate Authority Certificate (SHA-1 Fingerprint:
E2:FB:30:09:53:90:9A:31:30:C3:F0:07:8F:64:65:CD:11:0A:1A:A2)
saved in file "c:\intersystems\myinstnace\mgr\MyCA.cer"
```

- To download any certificate that the CA has issued — including any certificate for the CA client itself, you can locate the certificate by its serial number, the name of the host of the CA client (the **Hostname** column), the name of the instance of the CA client (the **Instance** column), or the root file name of the certificate (the **Filename** column).
- To view any certificates issued for the current instance, click **Show Certificates for This Instance**. This displays a table of certificates from which you can download a certificate, listing only the **Serial Number** and **Filename** columns.

3. When you click **Get** to download a certificate, InterSystems IRIS displays a confirmation message, such as

```
Certificate number 74 (SHA-1 Fingerprint:
45:E8:DE:0C:15:BF:A7:89:58:04:5E:68:2E:4D:BB:01:F5:90:94:97)
saved in file "c:\intersystems\myinstance\mgr\IstanbulAcctsPayable.cer"
```

While InterSystems IRIS initially downloads certificates to the manager’s directory, once they are on the client host, you can move them anywhere.