

## Client Public/Private Key Instructions

***For B2B Requests:*** In addition to the instructions below, please complete the **Application Access Request Form (AARF)** at <http://www.caiso.com/docs/2000/03/01/2000030110195926538.xls> to include the device type, device name, applications, roles, and environments required.

***For Server/Device certificates:*** In addition to the instructions below, please complete the **Application Access Request Form (AARF)** at <http://www.caiso.com/docs/2000/03/01/2000030110195926538.xls> to include the device type, device name and environments required.

### **Background Information**

Given the confidential nature of communications between CAISO and External Organizations, client authentication is preferred using standard x.509v3 certificates. CAISO's Public Key Infrastructure (PKI) issues these certificates, which ultimately chain to a single root certification authority, thus enabling trust between the client and the server. There are essentially two parts to the x.509v3 client certificate<sup>1</sup>: a private key and a public key. For the security of the connecting entity, it is a good security practice to generate the private key on the client site (stored in a physically secure location), instead of having CAISO generate the private key on behalf of the entity. With this in mind, the following procedures have been created to assist entities with generating the appropriate types of keys and certificate signing requests (CSR) so that their systems can utilize CAISO's certificates in a manner consistent with the Certificate Policy (CP) and Certificate Practice Statements (CPS). These documents ("CA ISO Certificate Policies v2.1" and "CA ISO Certification Practice Statement v2.1 for Basic Assurance Certification Authority (CA)") can be located and reviewed at the following website location:

<http://www1.caiso.com/pubinfo/info-security/cps/index.html>

### **Software to Generate Keys and CSRs**

Using Existing Software for Key/CSR Generation

Depending on the type of server that you are running, you may have the ability to generate a set of server keys and certificate requests from a specific application running on your system. For example, if the system is running a Sun, IIS or Apache web server, the ability to generate the required keys and certificates are built into the product. Following are the specifications needed to generate your private key and certificate signing requests for these types of servers:

#### **Key generation specifics:**

- Generate RSA keys
- Key length should be a **minimum of 1024 bits**

---

<sup>1</sup> The private key is not in the certificate. However, the certificate includes the public key, which is closely related to the private key.

- Store the private key securely, for example by encrypting it using either 3DES or RC4 encryption.

### **Certificate Signing Request (CSR) specifics:**

- The common name (CN) should reflect the server's DNS host name
- A CSR is required for each server that will establish a connection.
- The CSR should be generated according to the Public Key Cryptography Standard #10 (PKCS #10) and delivered to CAISO (as detailed later in this document).

### **Using OpenSSL to generate keys and certificates**

If your current system configuration is not technically capable of generating keys and CSRs, you will need to install and use an application that can do so. One such application that is commonly used is OpenSSL. Please see [www.openssl.org](http://www.openssl.org) for additional details.

If you are utilizing the OpenSSL program, following are the associated commands that will produce the types of keys and CSRs sufficient for CAISO's requirements:

#### **To generate a new key:**

**openssl genrsa -des3 -out <filename>.key 1024**

For example, the following command generates a 1024 bit RSA key and stores it in the file myServer.key. The file's content is encrypted via the 3DES algorithm, using a key that is derived from the password provided by the user.

**openssl genrsa -des3 -out myServer.key 1024**

#### **To generate a new certificate signing request:**

**openssl req -config <config\_file\_name> -new -key <filename>.key -out <filename>.csr**

For example, the following command generates a PKCS #10 CSR request using the key that was create previously and stored in the file myServer.key. The CSR is stored in a file called myServerP10.csr. Note that OpenSSL comes with a default configuration file that is suitable for most cases. OpenSSL uses this file to determine (among other things) how to form the CSR.

**openssl req -config openssl.cnf -new -key myServer.key -out myServerP10.csr**

Once your CSR is generated, you will need to submit it to CAISO for signing along with a completed Application Access Request Form (AARF). Please forward these items to [certrequest@caiso.com](mailto:certrequest@caiso.com). The standard SLA associated with certificates is ten business days from the time the request is approved and a task is assigned to CAISO's Information Security Department to issue the certificate. Please contact the CAISO Help Desk at 888-889-0450 if you do not receive your certificate within this timeframe.

After receiving your certificate (essentially your certified public key), you will need to install CAISO's trusted root certificates. These can be downloaded at <http://www1.caiso.com/pubinfo/info-security/certs/index.html>. Depending on which type of systems you are working with, production or non-production, you will need to download the appropriate certificate chain: CAISO\_ROOT\_CA, and CAISO\_ISSUING\_CA for production; or CAISO\_ROOT\_CA and CAISO\_TEST\_CA for non-production.

### **PKCS12 File Creation**

If you require a PKCS12 file, please use the command below. Please note that the PEM encoded file indicated in “-certfile <filename>.pem” needs to be a concatenated file with CAISO's three trusted root certificates (CAISO\_ROOT\_CA, and CAISO\_ISSUING\_CA for production certificates, or CAISO\_ROOT\_CA and CAISO\_TEST\_CA for non-production certificates). The root certificates can be obtained from <http://www1.caiso.com/pubinfo/info-security/certs/index.html>.

```
openssl pkcs12 -export -in file.crt -inkey <filename>.key -certfile <filename>.pem  
-out <file>.p12
```

For example, the following command creates a PKCS12 file called myServer.p12 from the private key file myServer.key, the certificate that was issued to you in file called myServer.crt and all of CAISO CAs's certificates in a file called CAISOCerts.pem.

```
openssl pkcs12 -export -in myServer.crt -inkey myServer.key -certfile CAISOCerts.pem -  
out myServer.p12
```

### **Using Java keytool to generate keys and CSRs**

If your system is Java based and can leverage a Java key store, you may use the **keytool** command to generate keys and CSRs as well as install certificates. Please use the following command to see the available options for `keytool`.

```
keytool -help
```

The following sets of commands illustrate how you may use `keytool`. To generate an RSA key pair in a key store called *myServerStore*, use the following command. Note that the key is given the name (a.k.a., alias) *myServerKey* and also assigned a distinguished name *cn=Server.example.com*.

```
keytool -keystore myServerStore -genkey -alias myServerKey  
-keyalg RSA -keysize 1024 -dname "cn=myServer.example.com"
```

The following command creates a CSR using the private key that was generated in the previous example. This command exports the CSR to a file called *myServerP10.csr*.

```
keytool -keystore myServerStore -certreq -alias myServerKey  
-file myServerP10.csr -sigalg sha1WithRSA.
```

Once your CSR is generated, you will need to submit it along with a completed Application Access Request Form (AARF) to CAISO for signing. Please forward the request to [certrequest@caiso.com](mailto:certrequest@caiso.com)

. The standard SLA associated with certificates is ten business days from the time the request is approved and a task is assigned to CAISO's Information Security Department to issue the certificate. Please contact the CAISO Help Desk at (888) 889-0450 if you do not receive your certificate within this timeframe.

After receiving your certificate (essentially your certified public key), you will need to install CAISO's trusted root certificates. These can be downloaded at <http://www1.caiso.com/pubinfo/info-security/certs/index.html>. Depending on which type of systems you are working with, production or non-production, you will need to download the appropriate certificate chain: CAISO\_ROOT\_CA, and CAISO\_ISSUING\_CA for production, or CAISO\_ROOT\_CA and CAISO\_TEST\_CA for non-production.

### **Importing certificates to the Java key store**

Use the following procedures for importing your certificate along with CAISO's CA certificates to your Java key store.

To import CAISO's root PKI certificate, execute the following command. This example assumes that you have downloaded this certificate and stored it in a file called *caiso\_root.cer*.

```
keytool -keystore myServerStore -import -trustcacerts -  
alias CAISO_ROOT_CA -file caiso_root.cer
```

Repeat the above procedure for two other CAISO's certificate authorities. This example assumes that you have downloaded these certificates and stored them in files called *caiso\_issuing.cer* and *caiso\_test.cer* respectively.

```
keytool -keystore myServerStore -import -trustcacerts -  
alias CAISO_ISSUING_CA -file caiso_issuing.cer
```

```
keytool -keystore myServerStore -import -trustcacerts -  
alias CAISO_TEST_CA -file caiso_test.cer
```

As a last step, import the your server's certificate, which CAISO issued to you, and associate it with the private key that was generated previously. Assuming that your server's certificate is in a file called *myServer.cer*, then the following command imports the certificate your server's Java key store.

```
keytool -keystore myServerStore -import -alias myServerKey  
-file myServerP.cer
```

You can now use `keytool` to list all the certificates in your key store as illustrated below.

```
keytool -v -list -keystore myServerStore
```

## Using IIS to generate keys and certificates

### Important

You must be a member of the Administrators group on the local computer to perform the following procedure or procedures.

Procedures

### To obtain a server certificate from a third-party certification authority

- 1.) In IIS Manager double-click the local computer, and then double-click the **Web Sites** folder.
- 2.) Right-click the Web site or file for which you want to request a certificate, and then click **Properties**.
- 3.) On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
- 4.) In the Web Server Certificate Wizard, on the **Delayed or Immediate Request** page, click **Prepare the request now, but send it later**. By default, the certificate request file is saved as C:\Certreq.txt, but the wizard allows you to specify a different location.
- 5.) Complete the rest of the steps in the Web Server Certificate Wizard and then click **Finish**.
- 6.) Once your CSR is generated, you will need to submit it, along with the completed Application Access Request Form (AARF) to CAISO for signing. Please forward the request to [certrequest@caiso.com](mailto:certrequest@caiso.com). The standard SLA associated with certificates is ten business days from the time the request is approved and a task is assigned to CAISO's Information Security Department to issue the certificate. Please contact the CAISO Help Desk at (888) 889-0450 if you do not receive your certificate within this timeframe.

After receiving your certificate (essentially your certified public key), you will need to install CAISO's trusted root certificates. These can be downloaded at <http://www1.caiso.com/pubinfo/info-security/certs/index.html>. Depending on which type of systems you are working with, production or non-production, you will need to download the appropriate certificate chain: CAISO\_ROOT\_CA, and CAISO\_ISSUING\_CA for production, or CAISO\_ROOT\_CA and CAISO\_TEST\_CA for non-production.

### Installing Server Certificates (IIS 6.0)

After you have obtained a server certificate, you can install it. When you use the Server Certificate Wizard to install a server certificate, the process is referred to as *assigning* a server certificate.

### Important

You must be a member of the Administrators group on the local computer to perform the following procedure or procedures.

## Procedures

### To install a server certificate using the Web Server Certificate Wizard

- 1.) In IIS Manager expand the local computer, and then expand the **Web Sites** folder.
- 2.) Right-click the Web site or file that you want, and then click **Properties**.
- 3.) On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
- 4.) In the Web Server Certificate Wizard, click **Assign an existing certificate**.
- 5.) Follow the Web Server Certificate Wizard, which will guide you through the process of installing a server certificate.

## Note

When you use the Web Server Certificate Wizard to assign a certificate, you must specify a password before the certificate can be assigned to your Web server.