

CAISO Access FAQs

Numerous questions have been raised regarding access and certificate requests during discussions related to MRTU cutover. Below are frequently asked questions and CAISO's answers, as well as some definitions that may add clarification to related terminology.

All Application Access Request Forms (AARFs) can be obtained from the following link:

<http://www.caiso.com/pubinfo/info-security/certs/>. MRTU Production access forms are under the "Forms", "MRTU Production Forms" section. For the following MRTU related access requests, please use the forms indicated:

- User Certificates- "[MRTU Application Access Request/Change Form](#)"
- Integration Certificates- "[MRTU Production Integration Access Request Form](#)"
- Secure File Transfer Protocol (SFTP) Certificates- "[MRTU Application Access Request/Change Form](#)"

Application Access

Access to applications involves multiple components:

- 1) **Authentication**, typically performed with a digital certificate, provides the user's identity (a user can be a human or system), and;
- 2) **Authorization**, which defines access privileges for users.

While certificates provide the identity of a user, production-level certificates can be used across multiple environments, including Market Simulation and Production. While this is true, access permissions may vary between environments. Due to this fact, CAISO requested production access requests to be submitted prior to MRTU Go-Live for all individuals and systems.

User Certificates

A user certificate is a certificate issued to a named user for the purpose of accessing CAISO applications through a graphical user interface. These certificates contain the user's first name and last name. A user certificate is required for every user that needs access.

Q: Can I use a user certificate to access the business-to-business (B2B) application programming interface (API)?

A: Yes. If there is a user associated with the B2B call, then a user certificate can be used. This means that a user must activate the call to the B2B interface when it is invoked. If the B2B call is automated then an integration certificate should be used instead of a user certificate.

Integration Certificates

An integration certificate is a certificate issued to an organization for the purpose of integrating systems through an API. These certificates have the same attributes as user certificates, but are issued to the organization. A single integration certificate is required for each organization, per environment, integrating with CAISO.

Q: What is the purpose of an integration certificate?

A: An integration certificate is to identify the organization involved in transactions between external participant systems and CAISO systems.

Q: Is a MRTU Production Integration certificate required before go-live?

A: Yes, the CAISO will issue an organization-level certificate for integration.

Q: What if our system design presents an undue difficulty in transitioning to the integration certificate?

A: Participant issues preventing a transition to an integration certificate prior to go-live will be considered on a case-by-case basis. Please contact Leslie DeAnda at lideanda@caiso.com.

Q: What is the difference between an integration certificate and a device certificate?

A: In addition to the definitions provided for each, the process of requesting an integration certificate is different than the process for requesting a device certificate. To obtain a device certificate, Participants must generate their certificate keys and submit a Certificate Signing Request (CSR) to CAISO. CAISO will then return a certificate to the requesting Participant. To obtain an integration certificate, CAISO will generate and return all necessary components of the certificates without receiving a CSR. Please note that the process for BAPI and CRN SFTP access is different. For instructions please see <http://www.caiso.com/2044/2044bbdb4a5d0.pdf>.

Q: If we have multiple production systems that need to integrate with CAISO systems, will we need multiple integration certificates?

A: No, a single organization-level certificate will be required and can be installed on all systems integrating with CAISO systems through an API. The caveat is that non-production systems will require their own certificates for identification.

[Q: Our Company has regulatory requirements regarding access permissions between internal groups. How can this be addressed?](#)

[A: While a company will generally have integration certificates issued for production and non-production purposes, CAISO can generate certificates based on a group for organizations with this need.](#)

Q: When completing the MRTU Integration AARF, what should be indicated in the Common Name field?

A: The common name field should be populated with the name of organization requesting the certificate.

Q: Do we need to submit an access request form for any of the legacy applications, such as ADS or SLIC?

A: Current production users and systems will retain production access after MRTU Go-Live. Any changes to these systems will go through the standard "Application Access Request/Change Form", which can be located under "Production Forms (non-MRTU)" at the link above.

Q: Can I use an integration certificate to access the user interfaces?

A: No. Integration certificates can only be used for B2B API access.

[Q: Can backup integration certificates be provided for contingency purposes?](#)

[A: Yes, backup integration certificates can be provisioned for contingency purposes. Mainly, if the primary certificate's private key is compromised, which would require revocation, the backup certificate could be implemented immediately with minimal communication disruption.](#)

Device Certificates

A device certificate is a certificate issued to a specific device, such as a meter, RIG, or DPG, for the purpose of sending data directly to CAISO systems. A device certificate is required for each device sending data to the CAISO, but no changes are required for MRTU go-live.

SFTP Certificates

Q: How do we automate downloads from BAPI?

A: The BAPI SFTP system is available for system to system automated downloads. BAPI access is limited to 4 device and/or user accounts (which allows for backup accounts) for access to a given SC. An SSH RSA 2048bit public key is required for each user and can be created with most SFTP clients (See instructions - <http://www.caiso.com/1fac/1face13e69850.pdf>).

[Q: Can a single SFTP device certificate be used on multiple systems?](#)

[A: Device SFTP certificates can be installed on multiple servers within an organization.](#)

Q: How do we set up access for the CRN SFTP report?

A: The CRN SFTP system is available for user access to CRN reports. One public key per user is required. An SSH RSA 2048bit public key is required and can be created with most SFTP clients (See instructions - <http://www.caiso.com/2044/2044bbdb4a5d0.pdf>).

Market Notification System (MNS)

[Q: How many endpoints can we register to receive notifications?](#)

[A: An organization can register up to two \(2\) endpoints to receive MNS notifications; one for production and one for non-production.](#)

[Q: Will there be a market simulation MNS system in addition to a production MNS system after "Go-Live"?](#)

[A: There are currently plans for a single production MNS system. By selecting the current "Market Simulation" Notification Source, your registered endpoints will have access to MNS from Market Simulation into Production.](#)

General

Q: When are the MRTU Production User and Integration AARFs due?

A: These should be received by CAISO no later than T-60. If you have not returned the form, please do so as soon as possible. The requested certificate will be issued within two weeks of the date of receipt.

Q: When will the production only access be implemented?

A: The new production-only access date will be announced soon. This will not occur before T-60 or after T-30.

Q: Who should be indicated in the Contact Submitting form field of the MRTU AARFs?

A: Each company has a point of contact (POC) that is registered with CAISO. Each company's assigned POC must submit the requests. This ensures a consistent, streamlined process for access requests. If your company has not already submitted the Point of Contact Establishment form, requirements as well as the form can be obtained at <http://www.caiso.com/pubinfo/info-security/certs/>. If you have any questions



about this process, please contact Julia Payton at (916) 608-1133. These forms should be submitted by December 19th, 2008 to:

CAISO
Attn: Julia Payton
151 Blue Ravine Road
Folsom, CA 95630

Q: Our Company requires access to SCID data that is owned by one of our business partners. How is access approved in these situations?

A: The designated POC of the company that owns the data must submit the access request.

Q: Do we need a separate certificate for internet and ECN?

A: No certificates are valid across any interface that is available for the system.

If you have any additional questions, please contact Leslie DeAnda at lideanda@caiso.com .