PKI-Based Authentication Guide

Version 1.6

Development & Data Operations Department
PJM Interconnection

For Public Use

This page is intentionally left blank.

Contents

1.0 Overview

PJM is implementing Public Key Infrastructure (PKI) authentication to its OASIS & ExSchedule tools, via both graphical user interface (GUI) and Command Line Interface (CLI) access, as well as other PJM Tools transfers via CLI. With this implementation, users will now have to provide a certificate along with their normal PJM credentials.

1.1. PKI

PKI is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a specific user or device and is safe to use. These documents are known as certificates.

Most of the commonly asked questions about PKI are posted in the PKI FAQs document (PDF). If you still have more questions, or need guidance please contact Member Relations.

1.2. Background of Change

On Feb. 4, 2020, the Federal Energy Regulatory Commission (FERC) issued an order for public utilities to comply with the North American Energy Standards Board (NAESB) v3.2 of the Standards for Business Practices and Communication Protocols, which says to protect all OASIS transfers with certificate-based authentication. (refer to https://www.naesb.org/pdf4/ferc020420_final_rule_weq_v003.2_RM05-5_Order_No676-I.pdf)

1.3. Impacted Tools

PJM's OASIS and ExSchedule applications are impacted by the FERC order, so they will be the first applications utilizing PKI. PJM is planning to leverage the same solution to other tools utilizing browserless (aka, CLI) transfers that are part of the single sign-on (SSO) function in order to make them more secure.

Below is the list of impacted tools.

UI & Browserless/CLI	Browserless/CLI Only
ExSchedule	Markets Gateway*
OASIS	InSchedule*
	Power Meter*
	FTR Center*
	Capacity Exchange*
	DR Hub*
	MSRS (Refresh Version)*

* Customer may opt-in for browserless/CLI.

1.4. Definitions, Acronyms and Abbreviations

Acronym	Definition
PKI	Public Key Infrastructure
CA	Certificate Authority
Cert	Certificate
CAM	Company Account Manager

2.0 Certificate Management

2.1. General Rules

Both a user and a Company Account Manager (CAM) have the ability to upload the certificate to associate a certificate to the user's account. The user will need to provide the certificate each time they log in to the tool.

a. Users must obtain a certificate from one of the NAESB-approved Certificate Authorities (CA)

  i. NAESB-approved CAs also offers certificates that do not meet NAESB's parameters defined in WEQ012. A certificate must be NAESB compliant if a user wants to access ExSchedule/OASIS applications. Any users who do not have access to ExSchedule/OASIS applications may choose to use a non-NAESB compliant certificate.

b. Users can only upload the certificate for their own user accounts

c. CAMs can upload certificates to any user account

d. CAMs must approve a certificate uploaded by a user

e. Users need to install the certificate in a browser for browser-based access

f. Users need to provide the uploaded certificate each time they log in to the tool (for both browser and browserless transfers)

g. A certificate must be unique per user

PJM understands that with introduction of NAESB approved certificates, members will have greater responsibility to maintain each user account. PJM offers a Single-User-Multi-Account (SUMA) feature for members who have multiple accounts with PJM. Users can choose to maintain a single-user account that can access data across multiple accounts. Guidance for SUMA is available.

2.2. File-Type Restrictions

While uploading a certificate to a user account in Account Manager, only certificates that **do not contain** the private key are permitted. (e.g., *.*pem, *.*crt, *.*cer, *.*der, *.*cert)

When using browser and PJM's CLI method, a user must use a certificate file that **does contain** the private key. (e.g., *.*pfx, *.*p12)

2.3. Obtaining a Certificate

Only NAESB-approved CAs are supported for use with PJM PKI authentication. A user has to purchase a certificate from one of the below approved certificate authorities.

a. OATI (www.oati.com)

b. Systrends (www.systrends.com)

c. GlobalSign (www.globalsign.com)

d. SSL (www.ssl.com)

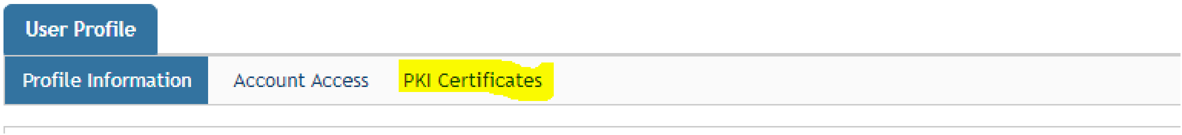
Note: If a user has access to OASIS and/or ExSchedule, then the certificate has to match the NAESB assurance level (https://www.naesb.org/weq/weq_standards.asp).

2.4. Linking Certificate (User)

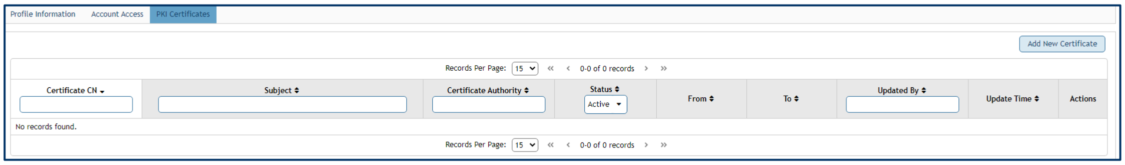
Users can follow the below steps to link the certificate to their user account.

a. Log in to Account Manager at accountmanager.pjm.com (accountmanagertrain.pjm.com for sandbox).

b. Click on User Profile, then PKI Certificates tab.

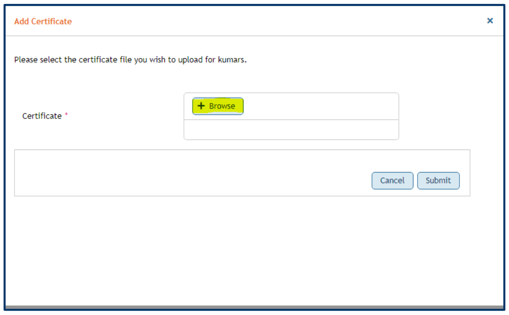


c. Click on Add New Certificate and select certificate from file upload window. Only public certificates are supported for upload (guidance on how to extract a public key from a certificate (PDF) is available).



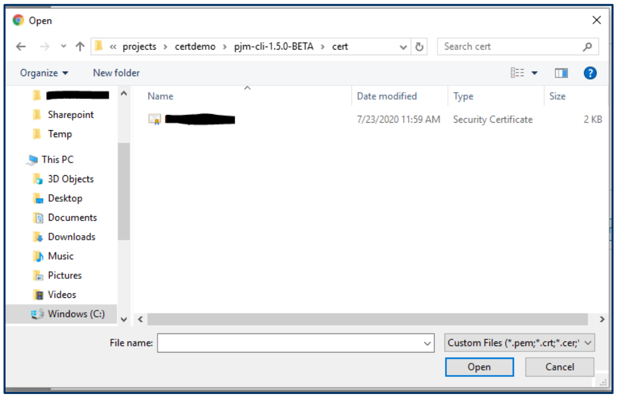
Certificate CN	Subject	Certificate Authority	Status	From	To	Updated By	Update Time	Actions
			Active					

No records found.



Please select the certificate file you wish to upload for kumars.

Certificate *



Name	Date modified	Type	Size
[redacted]	7/23/2020 11:59 AM	Security Certificate	2 KB

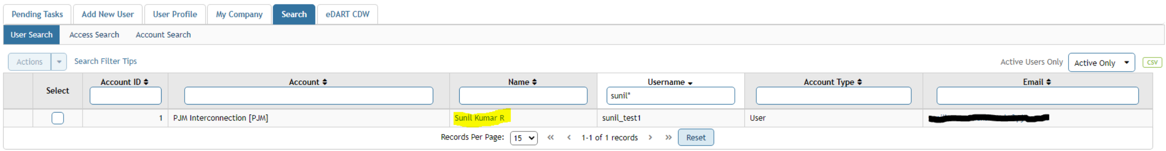
d. CAM **must** approve the uploaded certificate before a user can start using it.

2.5. Linking Certificate (CAM)

a. If the CAM is linking the certificate for a user, no additional approval is required.

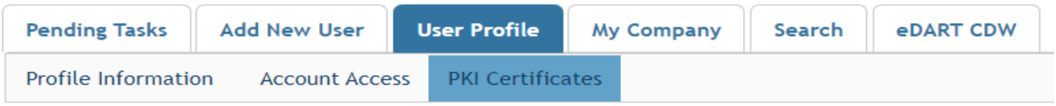
b. Log in to Account Manager at accountmanager.pjm.com (accountmanagertrain.pjm.com for sandbox).

c. Click on Search tab, and then click on User Search tab. To edit, click on the name link.

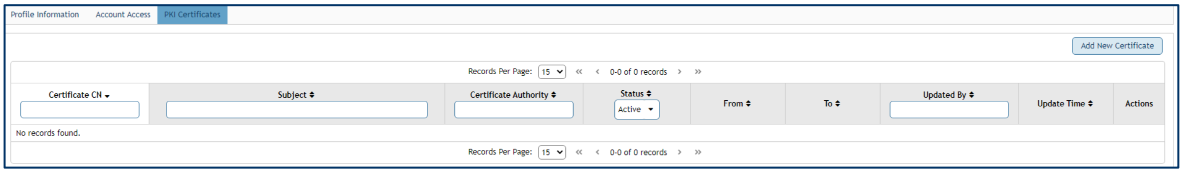


Select	Account ID ⬍	Account ⬍	Name ⬍	Username ▾	Account Type ⬍	Email ⬍
				sunil*		
□	1	PJM Interconnection [PJM]	Sunil Kumar R	sunil_test1	User	[redacted]

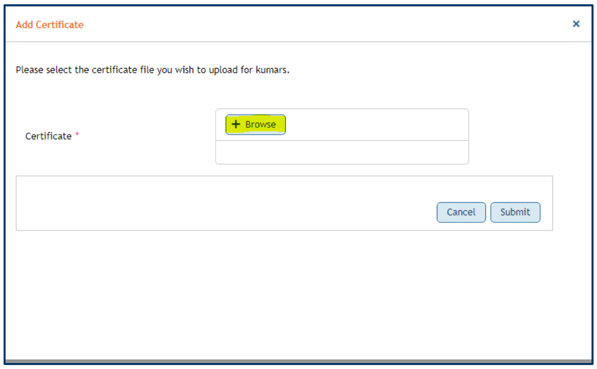
d. Click on PKI Certificates tab.



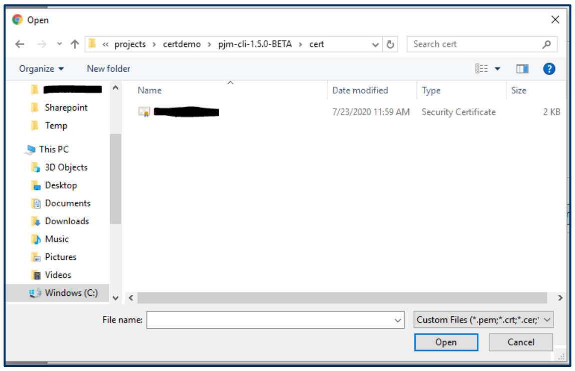
e. Click on Add New Certificate and select certificate from file upload window. Only public certificates are supported for upload (guidance on [how to extract a public key from a certificate](#) (PDF) is available).



Certificate CN ▾	Subject ⬍	Certificate Authority ⬍	Status ⬍	From ⬍	To ⬍	Updated By ⬍	Update Time ⬍	Actions
			Active					
No records found.								



Please select the certificate file you wish to upload for kumars.



[redacted]

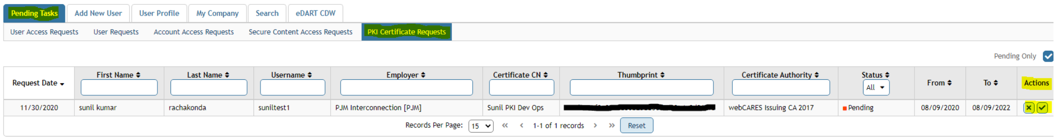
Name	Date modified	Type	Size
[redacted]	7/23/2020 11:59 AM	Security Certificate	2 KB

2.6. CAM Approving Certificate Linkage

a. Log in to Account Manager at accountmanager.pjm.com (accountmanagertrain.pjm.com for sandbox).

b. Click on Pending Tasks, then PKI Certificate Requests tab.

c. From Actions, the CAM can choose to Approve or Decline the request.



Request Date	First Name	Last Name	Username	Employer	Certificate CN	Thumbprint	Certificate Authority	Status	From	To	Actions
								All			
11/30/2020	sunil kumar	rachakonda	suniltest1	PJM Interconnection [PJM]	Sunil PKI Dev Ops	[redacted]	webCARES Issuing CA 2017	Pending	08/09/2020	08/09/2022	☒ ☑

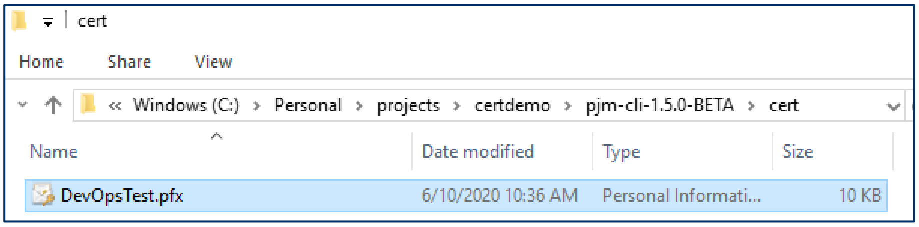
Records Per Page: 15 « ‹ 1-1 of 1 records › » Reset

2.7. Installing the Certificate within the Browser

The instructions below detail how to install a PFX certificate within Internet Explorer, Edge and Chrome browsers.

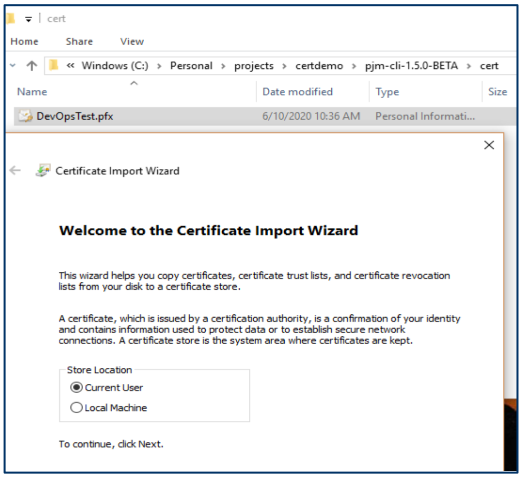
a. Double-click on the certificate PFX file and follow the steps within the Certificate Import Wizard, selecting the default options in Steps 1 through 3. At Step 4, users will need provide the certificate password.

Step 1.


cert
Home
Share
View
« Windows (C:) › Personal › projects › certdemo › pjm-cli-1.5.0-BETA › cert

Name	Date modified	Type	Size
DevOpsTest.pfx	6/10/2020 10:36 AM	Personal Informati...	10 KB

Step 2.


cert
Home
Share
View
« Windows (C:) › Personal › projects › certdemo › pjm-cli-1.5.0-BETA › cert
Name
Date modified
Type
Size
DevOpsTest.pfx
6/10/2020 10:36 AM
Personal Informati...
Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

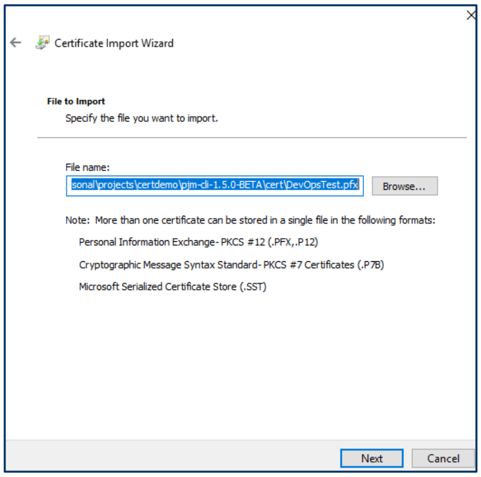
Store Location

● Current User

○ Local Machine

To continue, click Next.

Step 3.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:
sonal\projects\certdemo\pjm-cli-1.5.0-BETA\cert\DevOpsTest.pfx

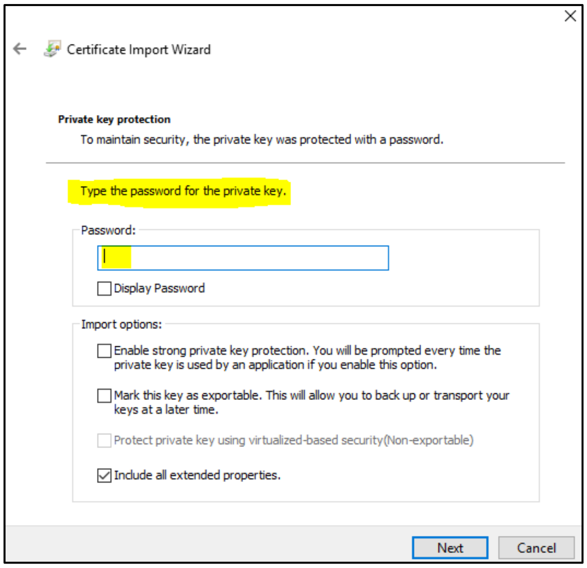
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Step 4.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Display Password

Import options:

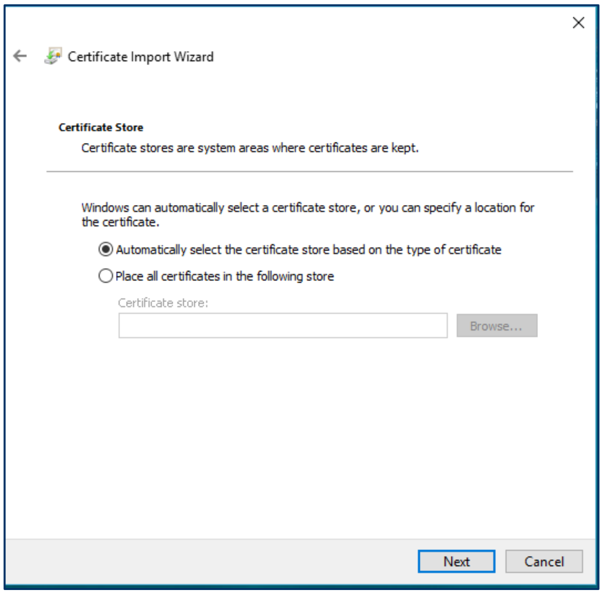
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

Step 5.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

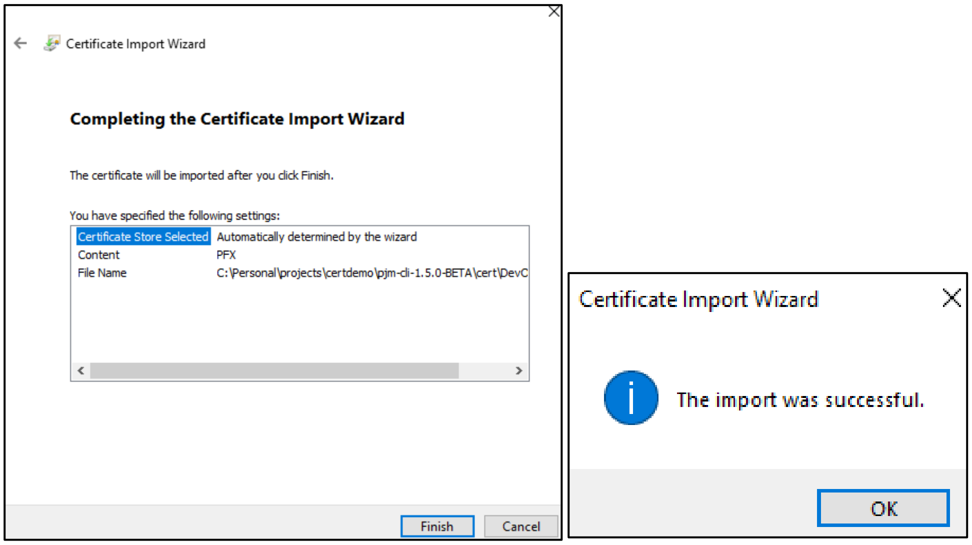
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Step 6.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\Personal\projects\certdemo\pjm-cli-1.5.0-BETA\cert\DevC

Certificate Import Wizard

The import was successful.

2.8. Certificate Renewal

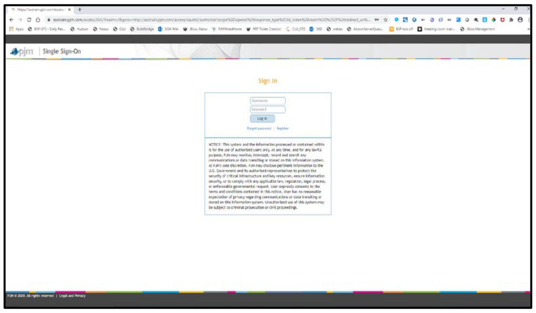
Certificates are normally valid for one to two years. Users should plan to purchase new certificates before current ones expire to maintain uninterrupted access to tools. Users can follow the same process for setting up new certificates as listed in sections 2.1 through 2.7. Once a new certificate is setup and the user is able to access the tools, users can delete old certificates from the account manager PKI certificate tab and from their machine.

3.0 Log in to PJM Tools – Via Browser

Logging in to a PJM PKI-based application is a two-step authentication process. Users will need to provide their user credentials and then will be presented with the certificate prompt. Below are the steps to log in.

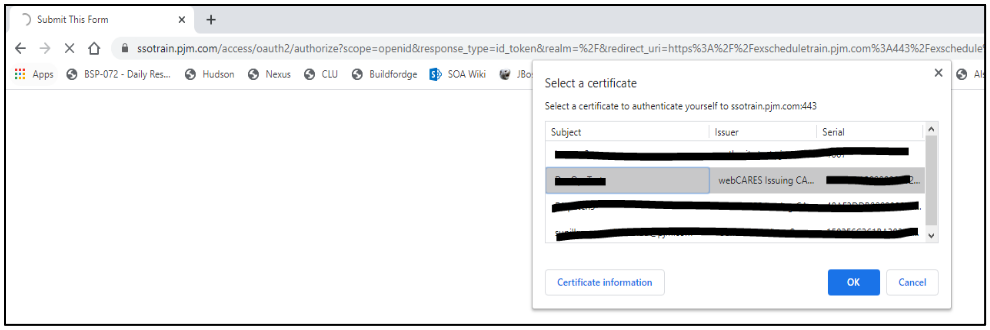
a. From the browser, enter the application URL (e.g., https://exschedule.pjm.com).

b. The SSO will prompt for user credentials. Enter the username and password.


pjm | Single Sign-On
Sign In
Username
Password
Log In
Forgot password | Register
PJM © 2020. All rights reserved | Legal and Privacy

NOTICE: This system and the information processed or contained within is for the use of authorized users only. At any time, and for any lawful purpose, PJM may monitor, intercept, record and search any communications or data transiting or stored on this information system. At PJM's sole discretion, PJM may disclose pertinent information to the U.S. Government and its authorized representatives to protect the security of critical infrastructure and key resources, ensure information security, or to comply with any applicable law, regulation, legal process, or enforceable governmental request. User expressly consents to the terms and conditions contained in this notice. User has no reasonable expectation of privacy regarding communications or data transiting or stored on this information system. Unauthorized use of this system may be subject to criminal prosecution or civil proceedings.

c. After the credentials are validated, users will be prompted to select a certificate. Select the certificate name of the one previously uploaded to Account Manager.


Submit This Form
ssotrain.pjm.com/access/oauth2/authorize?scope=openid&response_type=id_token&realm=%2F&redirect_uri=https%3A%2F%2Fexscheduletrain.pjm.com%3A443%2Fexschedule
Apps
BSP-072 - Daily Res...
Hudson
Nexus
CLU
Buildfordge
SOA Wiki
Certificate information
OK
Cancel

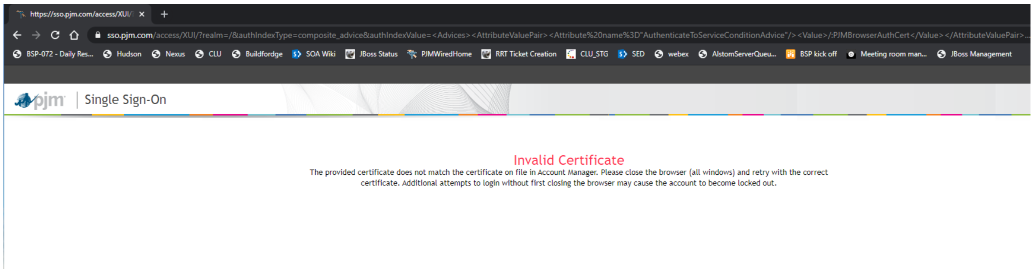
Select a certificate

Select a certificate to authenticate yourself to ssotrain.pjm.com:443

Subject	Issuer	Serial
[redacted]		
[redacted]	webCARES Issuing CA...	[redacted]
[redacted]		
[redacted]		

d. After the certificate is validated, users will be redirected to the PJM application.

e. In case of an incorrect certificate, users will be redirected to an error page. The browser does cache certificate selections, so users will **need close all tabs/windows before retrying**. After four consecutive attempts of selecting an invalid certificate, the account will be locked. The user must contact their CAM to unlock it.


https://sso.pjm.com/access/XUI/
sso.pjm.com/access/XUI/?realm=/&authIndexType=composite_advice&authIndexValue=<Advices><AttributeValuePair><Attribute%20name%3D"AuthenticateToServiceConditionAdvice"/><Value>/:PJMBrowserAuthCert</Value></AttributeValuePair>...
BSP-072 - Daily Res...
Hudson
Nexus
CLU
Buildfordge
SOA Wiki
JBoss Status
PJMWiredHome
RRT Ticket Creation
CLU_STG
SED
webex
AlstomServerQueu...
BSP kick off
Meeting room man...
JBoss Management
pjm | Single Sign-On

Invalid Certificate

The provided certificate does not match the certificate on file in Account Manager. Please close the browser (all windows) and retry with the correct certificate. Additional attempts to login without first closing the browser may cause the account to become locked out.

4.0 Log in to PJM Tools – Via API

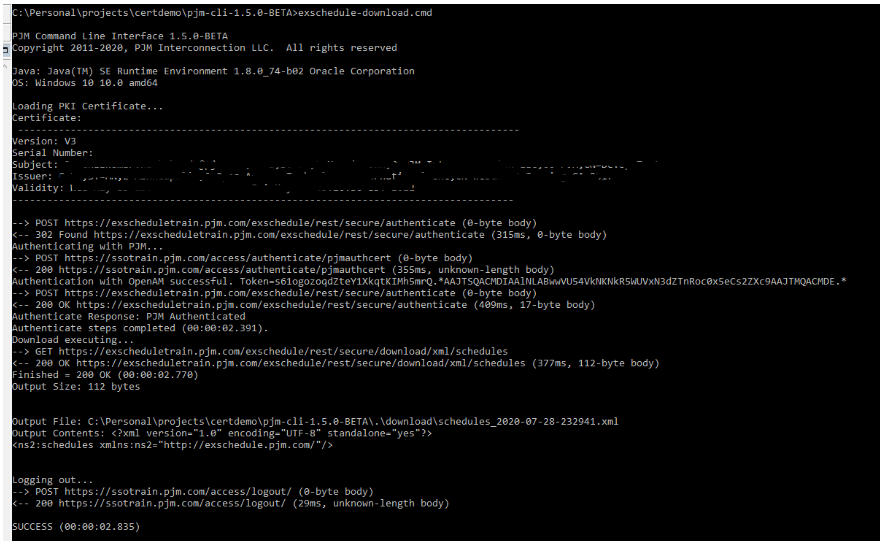
4.1. Command Line Interface – CLI

Users will need to use the Command Line Interface - Java 8+ or higher, which can be downloaded from https://pjm.com/markets-and-operations/etools/system-requirements.aspx.

Within the setenv.cmd file, a new property ‘`CERTIFICATE`’ has been added. Users need to update this property with the certificate location and certificate password, along with regular PJM username/password and Java location properties.

```
CERTIFICATE=-r "C:\filelocation\cert.pfx|ENC(encrypted password)"
```

There is no change on how to use the CLI tools. Users can refer to the *CLI User Guide* found within the pjm-command-line-interface-java-8.zip file located at: https://pjm.com/markets-and-operations/etools/system-requirements.aspx.



```
C:\Personal\projects\certdemo\pjm-cli-1.5.0-BETA>exschedule-download.cmd

PJM Command Line Interface 1.5.0-BETA
Copyright 2011-2020, PJM Interconnection LLC.  All rights reserved

Java: Java(TM) SE Runtime Environment 1.8.0_74-b02 Oracle Corporation
OS: Windows 10 10.0 amd64

Loading PKI Certificate...
Certificate:
 -------------------------------------------------------------------------------------
Version: V3
Serial Number:
Subject: [redacted]
Issuer: [redacted]
Validity: [redacted]
-------------------------------------------------------------------------------------

--> POST https://exscheduletrain.pjm.com/exschedule/rest/secure/authenticate (0-byte body)
<-- 302 Found https://exscheduletrain.pjm.com/exschedule/rest/secure/authenticate (315ms, 0-byte body)
Authenticating with PJM...
--> POST https://ssotrain.pjm.com/access/authenticate/pjmauthcert (0-byte body)
<-- 200 https://ssotrain.pjm.com/access/authenticate/pjmauthcert (355ms, unknown-length body)
Authentication with OpenAM successful. Token=s61ogozoqdZteY1XkqtKIMh5mrQ.*AAJTSQACMDIAAlNLABwwVU54VkNKNkR5WUVxN3dZTnRoc0x5eCs2ZXc9AAJTMQACMDE.*
--> POST https://exscheduletrain.pjm.com/exschedule/rest/secure/authenticate (0-byte body)
<-- 200 OK https://exscheduletrain.pjm.com/exschedule/rest/secure/authenticate (409ms, 17-byte body)
Authenticate Response: PJM Authenticated
Authenticate steps completed (00:00:02.391).
Download executing...
--> GET https://exscheduletrain.pjm.com/exschedule/rest/secure/download/xml/schedules
<-- 200 OK https://exscheduletrain.pjm.com/exschedule/rest/secure/download/xml/schedules (377ms, 112-byte body)
Finished = 200 OK (00:00:02.770)
Output Size: 112 bytes


Output File: C:\Personal\projects\certdemo\pjm-cli-1.5.0-BETA\.\download\schedules_2020-07-28-232941.xml
Output Contents: <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:schedules xmlns:ns2="http://exschedule.pjm.com/"/>


Logging out...
--> POST https://ssotrain.pjm.com/access/logout/ (0-byte body)
<-- 200 https://ssotrain.pjm.com/access/logout/ (29ms, unknown-length body)

SUCCESS (00:00:02.835)
```

4.2. Browserless Transfer

If users have custom code calling the PJM REST API, there is a change to the SSO authentication process. Users will need to establish a two-way SSL with the client certificate on the “access/authenticate/pjmauthcert” endpoint, along with credentials, to get an SSO token. The call to the application URL remains the same, and users will need to pass a token as a header. Below is a curl example:

Authentication:

```
curl --request POST --key testcert.key.pem --cert
‘testcert.crt:<privatekeypassword>' --header "X-OpenAM-Username: <sso_username>"
--header 'X-OpenAM-Password: <sso_password>'
'https://sso.pjm.com/access/authenticate/pjmauthcert‘
```

```
{"tokenId":“<tokenid>","successUrl":"/access/console","realm":"/"}
```

```
   * sotrain.pjm.com/access/authenticate/pjmauthcert is the url for Train
```

In the above curl example, we did pass a private key, public certificate and certificate password to establish a two-way SSL connection. Depending the tool/language/framework being used, it will change where some of them may need just a PFX file.

Application REST API:

```
curl --request GET --header "Cookie: pjmauth= <tokenid>”
‘https://exschedule.pjm.com/exschedule/rest/secure/download/xml/schedules’
```

Java code example is available.

.Net code example is available.

5.0 Opt-in for browserless Transfers

For PJM's OASIS and ExSchedule applications, PKI will be mandatory from the first day of implementation. For the rest of PJM's Tools, we will implement PKI in two phases: first optional, then mandatory.

During the optional phase, users can opt-in to PKI-based authentication by requesting access to a special role "Certificate Based Authentication Opt-In" from Account Manager. Afterwards, opt-in users have to provide a certificate for the tools below each time they access browserless transfers.

Markets Gateway
InSchedule
Power Meter
FTR Center
Capacity Exchange
DR Hub
MSRS (Refresh Version)

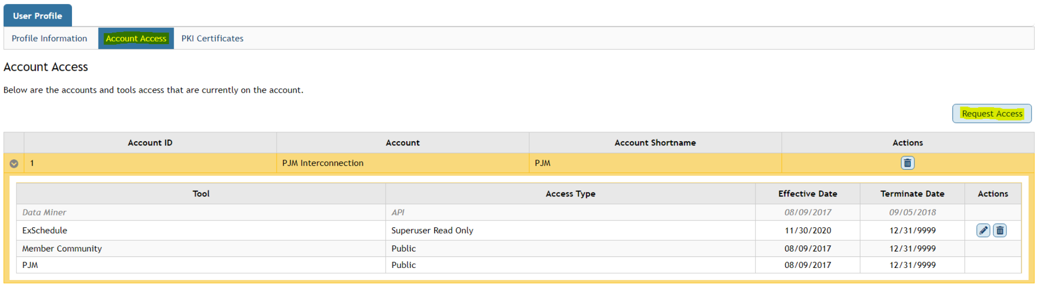
If for any reason users want to opt-out, they can work with their CAM to terminate access to the "Certificate Based Authentication Opt-In" role.

5.1. Requesting Opt-in from Account Manager

Users can follow the below steps to opt-in to certificate-based authentication.

a. Log in to the Account Manager application at accountmanager.pjm.com (accountmanagertrain.pjm.com for sandbox).

b. Click on Account Access, then Request Access.



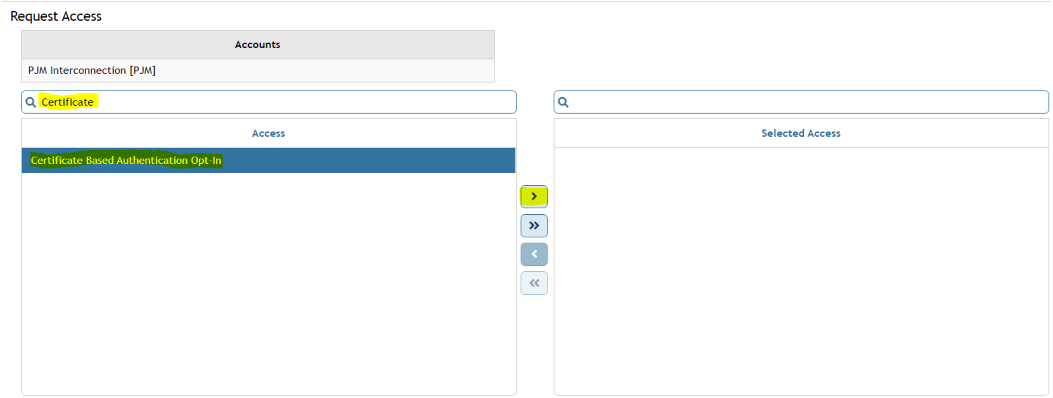
Account Access

Below are the accounts and tools access that are currently on the account.

Account ID	Account	Account Shortname	Actions
1	PJM Interconnection	PJM	

Tool	Access Type	Effective Date	Terminate Date	Actions
Data Miner	*API*	*08/09/2017*	*09/05/2018*	
ExSchedule	Superuser Read Only	11/30/2020	12/31/9999	
Member Community	Public	08/09/2017	12/31/9999	
PJM	Public	08/09/2017	12/31/9999	

c. Under request access select “Certificate Based Authentication Opt-In” from the access list, move the role to selected access and click the Next button.



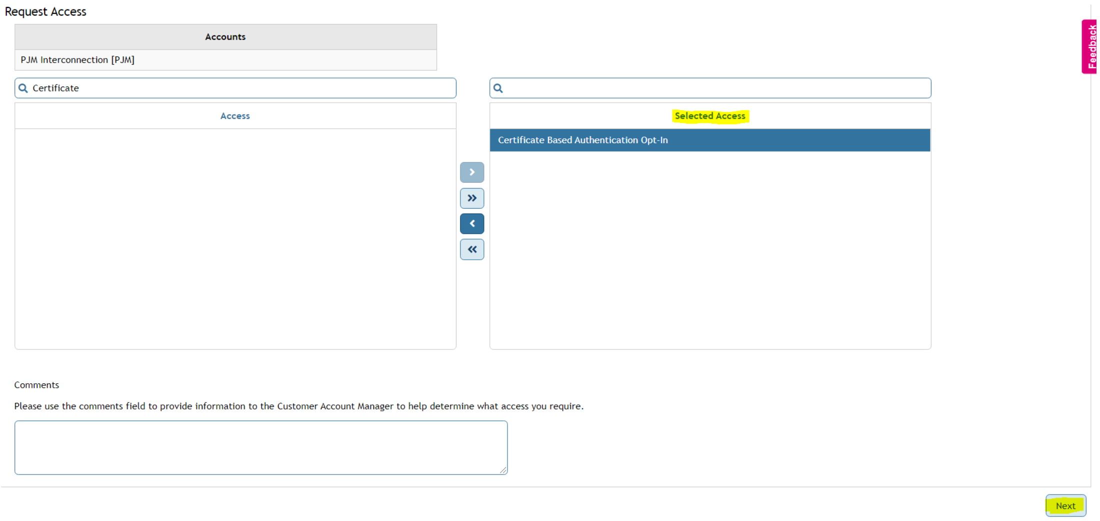
Request Access

Accounts
PJM Interconnection [PJM]

Search: Certificate

Access
Certificate Based Authentication Opt-In

Selected Access



Request Access

Accounts
PJM Interconnection [PJM]

Search: Certificate

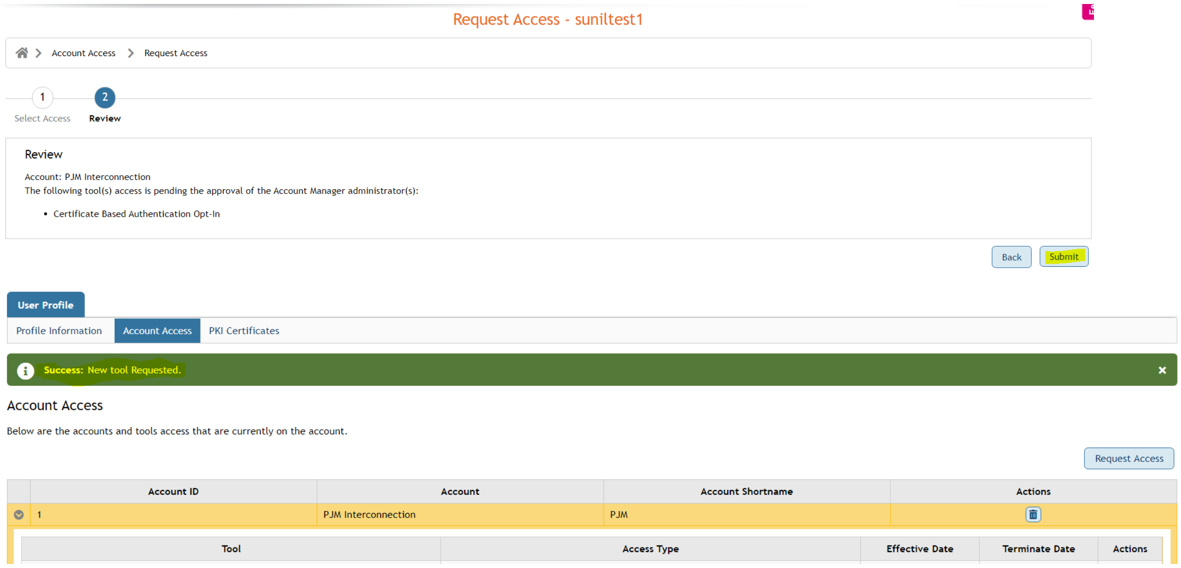
Access

Selected Access
Certificate Based Authentication Opt-In

Comments

Please use the comments field to provide information to the Customer Account Manager to help determine what access you require.

d. From the review page, click the Submit button.



Request Access - suniltest1

Account Access > Request Access

1 Select Access — 2 Review

Review

Account: PJM Interconnection

The following tool(s) access is pending the approval of the Account Manager administrator(s):

- Certificate Based Authentication Opt-In

Success: New tool Requested.

Account Access

Below are the accounts and tools access that are currently on the account.

	Account ID	Account	Account Shortname	Actions
⌄	1	PJM Interconnection	PJM	🗑

Tool	Access Type	Effective Date	Terminate Date	Actions

e. A CAM is required to approve the requested access and can follow same procedure when approving other roles.