Frequently Asked Questions about PKI Certificates and Two-Step Verification Browserless/API

Version: Mar. 3, 2021

Q **Why we are doing this?**

A On February 4, 2020 FERC issued an order for Public Utilities to comply with NAESB 3.2 standards which says to protect all OASIS transfers with Certificate based authentication.

Q **What is PKI?**

A Public Key Infrastructure (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 particular user or device and are safe to use. These documents are known as certificates.

Q **What applications are impacted with FERC order?**

A ExSchedule and OASIS (Both UI and Browserless)

Q **Will PJM use this solution anywhere else?**

A Yes, PJM is planning leverage same solution for browserless transfers that are part of single sign on(SSO), below are the impacted tools

- Markets Gateway (marketsgateway.pjm.com)
- InSchedule (insched.pjm.com)
- Power Meter (powermeter.pjm.com)
- FTR Center (ftrcenter.pjm.com)
- Capacity Exchange (capacityexchange.pjm.com)
- DR Hub (drhub.pjm.com)
- MSRS-Refreshed (msrsapp.pjm.com)

Q **Where can I get the PKI certificates?**

A Certificates must be purchased from NAESB approved certificate authorities, which are:

- OATI (www.oati.com)
- Systrends (www.systrends.com)
- GlobalSign (www.globalsign.com)
- SSL (www.ssl.com)

Q **Is the cost of the certificates covered by a PJM membership?**

A No, membership does not cover the cost of the certificate. Certificates must be purchased separately.

Q **Can I share the certificate with other users?**

A No, the certificate is unique to a user.

Q **How can I upload a certificate?**

A Users can upload the certificate from Account Manager User profile page. CAM has to approve the upload before user can start using it.

Q **Where can CAMs/ users find instructions on how to upload certificates in Account Manager?**

A PKI Guide is available at https://www.pjm.com/-/media/etools/security/pki-authentication-guide.ashx?la=en.

Q **Can I use a certificate with a .pfx prefix?**

A Pfx contains both public & private keys. PFX can be used only during login to tools application (e.g. OASIS) from browser/browserless. For uploading to Account Manager only public keys are supported. You can use openssl commands to extract the public keys, and save it in other formats like CER. Instructions are available at pki-export-public-keys

Q **How do I add the certificate to the browser?**

A Instructions are available at PKI Guide

Q **Do I need to add the certificate to the browser if I am only using browserless?**

A Not required.

Q **I have multiple usernames to access multiple accounts. Is there a solution available to condense the amount of usernames I use to reduce the amount of certificates need?**

A You can make use of the Single Use Multi Account (SUMA) feature. As a user when you have access to multiple accounts and sub accounts you can choose hold on to one single username and work with your CAM to make that one username a SUMA user. This will enable you to access multiple accounts with single user names. CAM can then terminate other obsolete usernames.

Q **If I have a SUMA username (one username with access to many subaccounts) can I use one certificate for the user?**

A Certificate is unique per user, with SUMA you will need to purchase only one certificate (not for each sub account).

Q **Can I have multiple certificates**

A Yes, you can upload multiple certificates through account manager, any one of them can be used during login.

Q **My certificate is about to expire, Can I upload the renewed certificate ahead of time?**

A Yes, you can upload ahead of time and start using new certificate right away. Remember you will also need to install the new certificate on your browser to use it. Your browser will show all active certificates that you have installed on your browser to pick. Remember if you have existing session open then you should end the session and close all browser windows or clear SSL state to get browser popup to select new certificate.

Q **Will you still need a username and password for browserless access?**

A Yes, you will still need a username and password along with the certificate.

Q **Will certificates used at other ISOs would work here?**

A Yes, certificates will work as long as they are from NAESB approved certificate authorities.

Q When will certificates be required?

A For ExSchedule and OASIS, they will be mandatory by the first quarter of 2021. For all other tools that use browserless transfers, they will be required sometime in 2021.

Q Are there any changes to the soft token for two-step verification?

A ExSchedule and OASIS will no longer require the soft tokens for two-step verification on the user interfaces. There will be no changes in the use of the soft token when accessing the user interface of all other applications.