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

Version: Jan. 10, 2022

Q What is PKI?

A Public Key Infrastructure (PKI) is a technology for authenticating users and devices in the digital world. PKI allows one or more trusted parties to digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device and is safe to use. These documents are referred to as certificates.

Q Why is PJM making this change?

A On Feb. 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 applications are impacted with the FERC order?

A ExSchedule and OASIS, since both use user interface (UI) and are browserless.

Q Will PJM make this change anywhere else? And if so, when?

A Yes. PJM is implementing the same solution for browserless only transfers that are part of single sign on (SSO). Below are the impacted tools and the dates they will be implemented.

- InSchedule ((insched.pjm.com) – July 13, 2022
- Power Meter (powermeter.pjm.com) – July 13, 2022
- FTR Center (ftrcenter.pjm.com) – June 28, 2022
- DR Hub (drhub.pjm.com) – September 21, 2022
- Capacity Exchange (capacityexchange.pjm.com) – June 28, 2022
- MSRS (msrsapp.pjm.com) – July 20, 2022

- Markets Gateway (marketsgateway.pjm.com) – August 28, 2022

Q Does a user need to add a certificate if the applications are accessed only through the user interface (UI)?

A No. This change is only for browserless access, except as mentioned for ExSchedule and OASIS, and where there is no certificate needed for the UI.

Q Does a user need to add a certificate if the applications are accessed through both user interface and browserless?

A Yes. This change impacts the browserless access making a certificate needed for access.

Q If a user does not upload a certificate prior to the mandatory dates, can the application still be accessed?

A Yes and no. The user will only be able to access the application through the user interface (UI), but will not be able to access the application via browserless. An error will be received.

Q Where can a user 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 my PJM membership?

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

Q Can a user share the certificate with other users?

A No, the certificate is unique to a user.

Q How can a user upload a certificate?

A Users can upload the certificate from their Account Manager User profile page. Their CAM has to approve the upload before it can be used.

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

A A PKI Guide. is available to guide the upload process.

Q Can a user use a certificate with a .pfx prefix?

A A PFX file contains both public and private keys. PFX can be used only during login to tools application (e.g., OASIS) that are browser/browserless. Only public keys are supported for upload into Account Manager. 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 does a user add the certificate to the browser?

A Instructions are available at PKI Guide.

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 to 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 a single user name. A 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 Certificates are unique per user, with SUMA you will need to purchase only one certificate (not for each sub account).

Q Can a user have multiple certificates?

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

Q Once a certificate is uploaded for a user, do they need to re-upload for each application?

A No. Once a certificate is uploaded to a user, that certificate applies to all applications the user has been granted access to use. A certificate will be applied automatically to any future applications accessed.

Q If a user uploads a certificate using the 'opt-in' process, does that certificate transfer over once the certificate is mandatory to use?

A Yes, and no further action is needed.

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. Remember, if you have existing session open then you should end the session and close all browser windows or clear the SSL state to get the browser pop-up to select a new certificate.

Q How will a user know if a certificate is about to expire?

A Account Manager will send a notification email to the user and CAM 30-days before the certificate expires.

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 work here?

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

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 for user interfaces. There will be no changes in the use of the soft token when accessing the user interface for all other applications.