



Tech Change Forum Special Session - Public Key Infrastructure (PKI) Educational Session

August 13, 2020

Sunil Rachakonda

- Due to feedback we've received, PJM is making some changes to further improve the user experience with the PKI implementation.
 - PKI Implementation times have been rescheduled
 - Browserless/API implementation have been rescheduled

Product - Action Required	Dates	Who May Be Affected
<p>Account Manager Train</p> <ul style="list-style-type: none"> Associate valid PKI certificates with user account in Account Manager 	<p>Dec 2020</p>	<ul style="list-style-type: none"> CAMs and users of ExSchedule and OASIS
<p>Train Implementation for ExSchedule & OASIS</p> <ul style="list-style-type: none"> Obtain valid PKI certificates from approved Certificate Authorities Rewrite Browserless/API authentication code Use PJM provided command line interface (CLI) 	<p>Dec 2020</p>	<ul style="list-style-type: none"> Users of ExSchedule and OASIS 3rd party Vendors for ExSchedule and OASIS Developers of ExSchedule and OASIS Browserless/API code



	2020						2021					
	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	June	July
PKI for OASIS & ExSchedule						Train ◆		Production: TBD ◆				
Browserless/API 2 Factor Authentication						Train ◆		Production (Opt-In): TBD ◆				

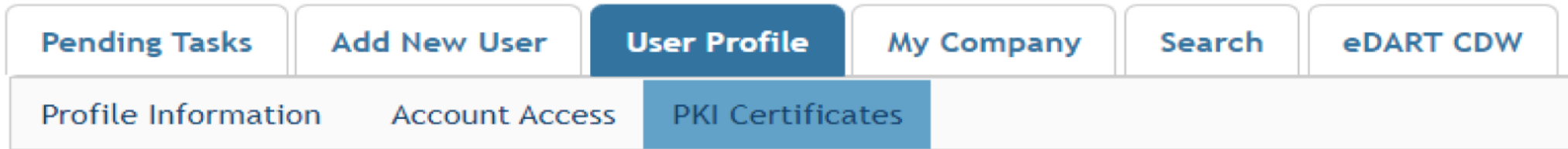
ExSchedule &
OASIS Public
Key Infrastructure
(PKI)

Browser-less/API
2 Factor
Authentication

- PKI
 - On February 4, 2020 FERC issued an order to comply with NAESB 3.2 changes
 - Implement PKI to provide secure access to
 - OASIS
 - E-Tagging applications (ExSchedule)
 - Existing certificates that meet NAESB requirements will be accepted
 - When:
 - Train: December, 2020
 - Production: Q1, 2021

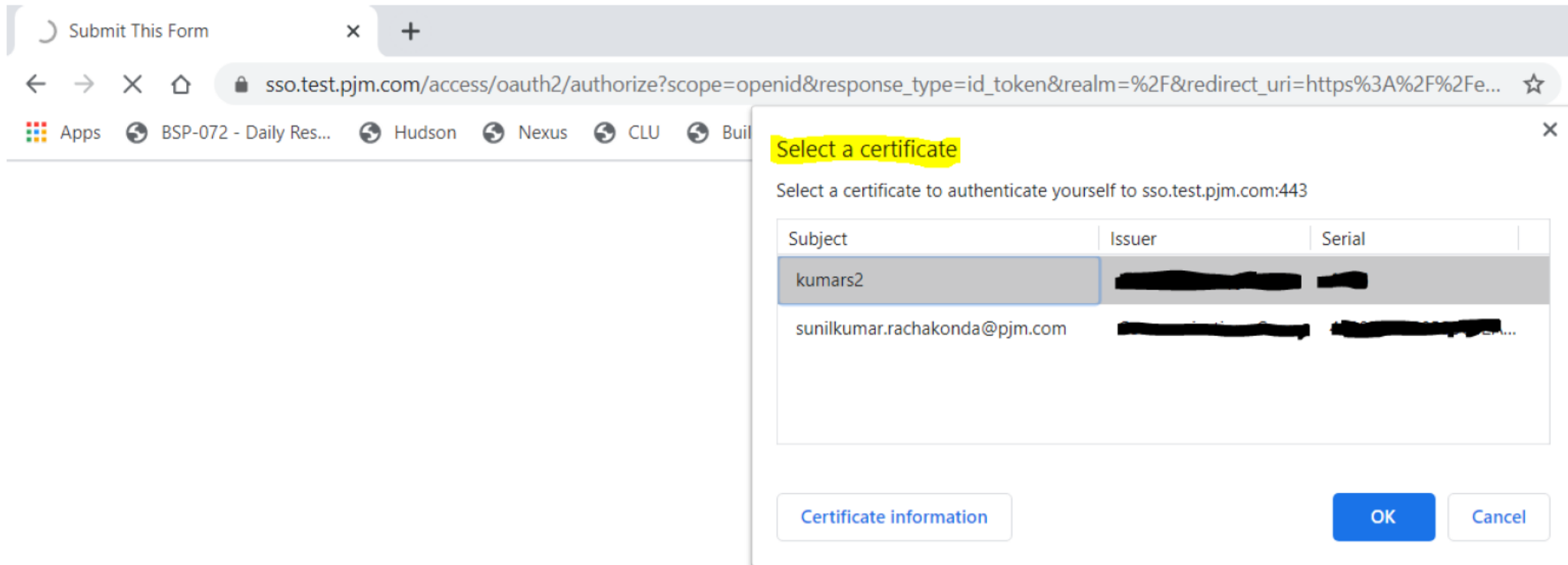
- Browserless/API 2 Factor Authentication
 - Leverage PKI solution
 - Scope
 - Included: All PJM Tools that are part of Single Sign On and have Browserless APIs
 - Excluded: ExSchedule and OASIS
 - Users can opt-in by requesting access to “Certificate Based Authentication Opt-In” role during optional period
 - When:
 - Optional in Q1, 2021
 - Mandatory later in 2021

- Uploading Certificate
 - The User can upload the certificate or the CAM can associate certificates with user account from Account Manager PKI Tab



- The CAM has to approve the certificate after the user upload
 - The user must Install the certificate in user's browser if logging into the UI

- Using certificate
 - On login to ExSchedule/OASIS the user will be prompted for a certificate



- Changes to Authentication process
- Associate certificates with user account from accountmanager PKI Tab
- Authenticate against 'sso.pjm.com/access/authenticate/pjmauthcert' with 2 way ssl connection (mutual authentication) to get a SSO token-id
- Call to Application REST API still same, pass token-id as header

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": "/"}
```

Application REST API

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

- New version 1.5.0
- Java version 8 Patch 165 or higher is required
- New user guide will be posted to PJM.COM
- No changes to usage of Application CLI commands
- A new property (below) was added to setenv.cmd file

```
set CERTIFICATE=-r “.pfx/.p12 file_location|privatekeypassword“
```

- <https://www.pjm.com/-/media/etools/security/pki-faqs.ashx?la=en>