Tools Security Roadmap

As of November 17, 2020

- Added Train release dates
- Added CAM approval page screen shot under Account Manager
- Added how to link for exporting public keys

Product - Action Required	Dates	Who May Be Affected
Account Manager Train • Associate valid PKI certificates with user account in Account Manager	**December 2** **4 p.m.**	• CAMs and users of ExSchedule and OASIS
Train Implementation for ExSchedule & OASIS • Obtain valid PKI certificates from approved Certificate Authorities • Rewrite Browserless/API authentication code • Use PJM provided command line interface (CLI)	**December 8** **4 p.m.**	• 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: Dec 8 ◆		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 8 at 4 p.m.
    - 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
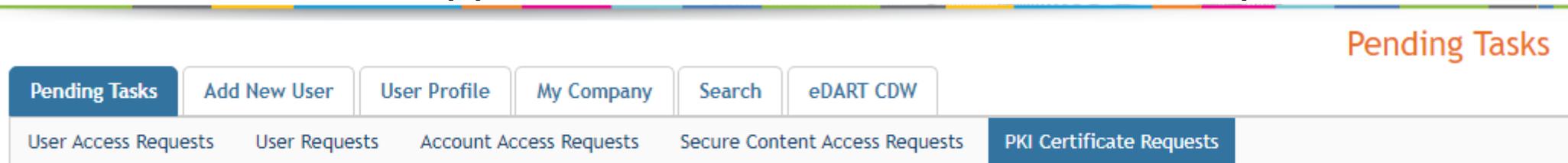
  - The user must Install the certificate in user's browser if logging into the UI

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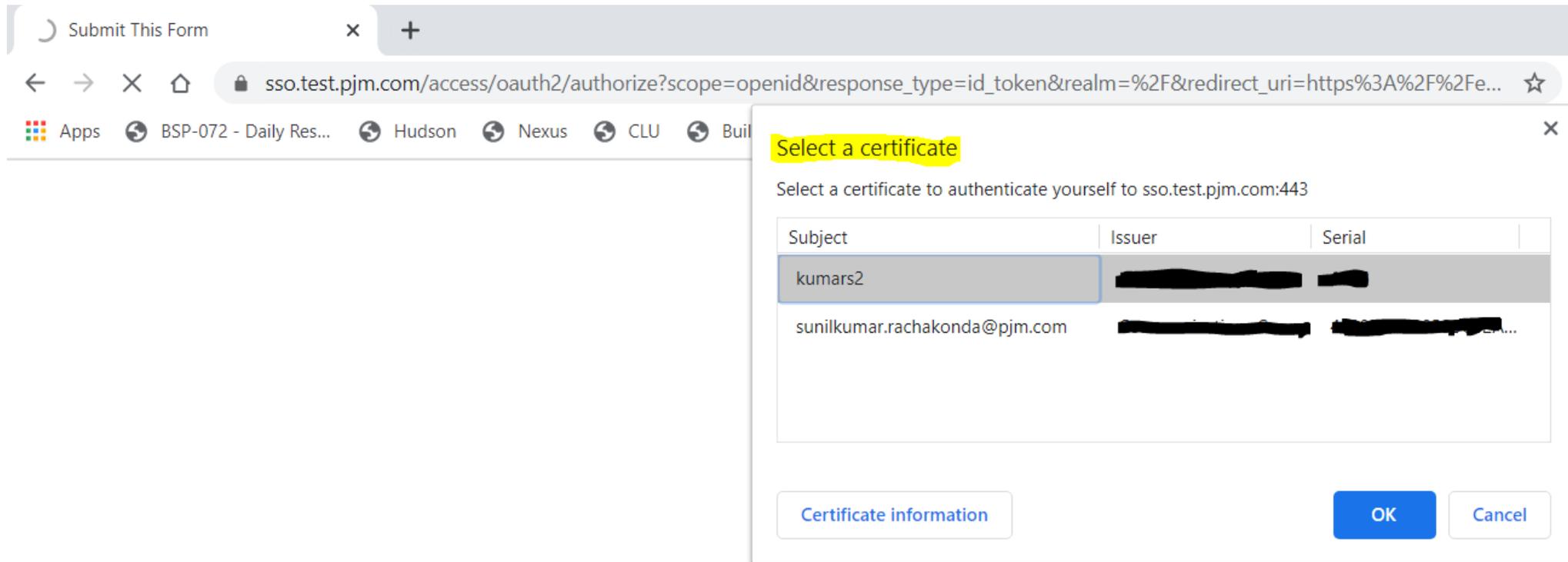
- Changes to Authentication process

- 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'
```

- Java Sample

  - https://www.pjm.com/-/media/etools/security/pki-certificate-authentication-java-code-sample.ashx?la=en

- .Net Sample

  - https://www.pjm.com/-/media/etools/security/pki-certificate-authentication-net-code-sample.ashx?la=en

- New version 1.5.0

- Java version 8 Patch 165 or higher is required

- Available at https://pjm.com/-/media/etools/pjm-command-line-interface-java-8.ashx?la=en

- 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"
  ```

- FAQs for PKI Certificates and Two-Step Verification Browserless/API: https://www.pjm.com/-/media/etools/security/pki-faqs.ashx?la=en

- PKI-Based Authentication Guide: https://www.pjm.com/-/media/etools/security/pki-authentication-guide.ashx?la=en

- Exporting public keys from pfx/p12 : https://www.pjm.com/-/media/etools/security/pki-export-public-keys.ashx?la=en