Tools Security Roadmap

As of September 15, 2020

Revisions

- None

Impact Details

Product - Action Required	Dates	Who May Be Affected
Account Manager Train • Associate valid PKI certificates with user account in Account Manager	**Dec 2020**	• 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)	**Dec 2020**	• Users of ExSchedule and OASIS • 3rd party Vendors for ExSchedule and OASIS • Developers of ExSchedule and OASIS Browserless/API code

2020-2021 Tentative Roadmap

	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 ◆				

Initiatives

ExSchedule & OASIS Public Key Infrastructure (PKI)

Browser-less/API 2 Factor Authentication

Background - PKI

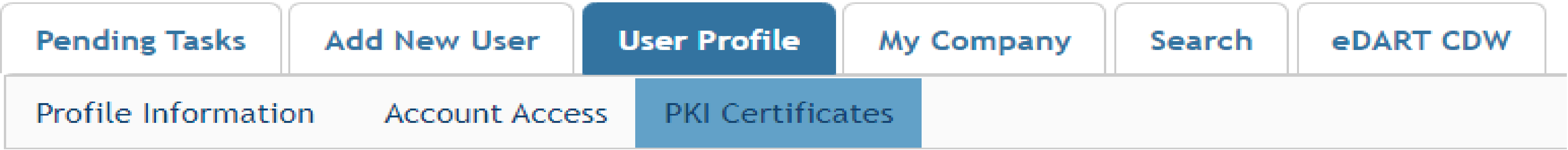
- PKI
  - On February 4, 2020 FERC issued an order to comply with NAESB 3.2 changes
  - Implement PKI to provide secure access to
    - OASIS
    - E-Tagging applications (ExSchedule)
  - Existing certificates that meet NAESB requirements will be accepted
  - When:
    - Train: December, 2020
    - Production: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

Background – Browserless/API 2 Factor Authentication

- 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

Account Manager

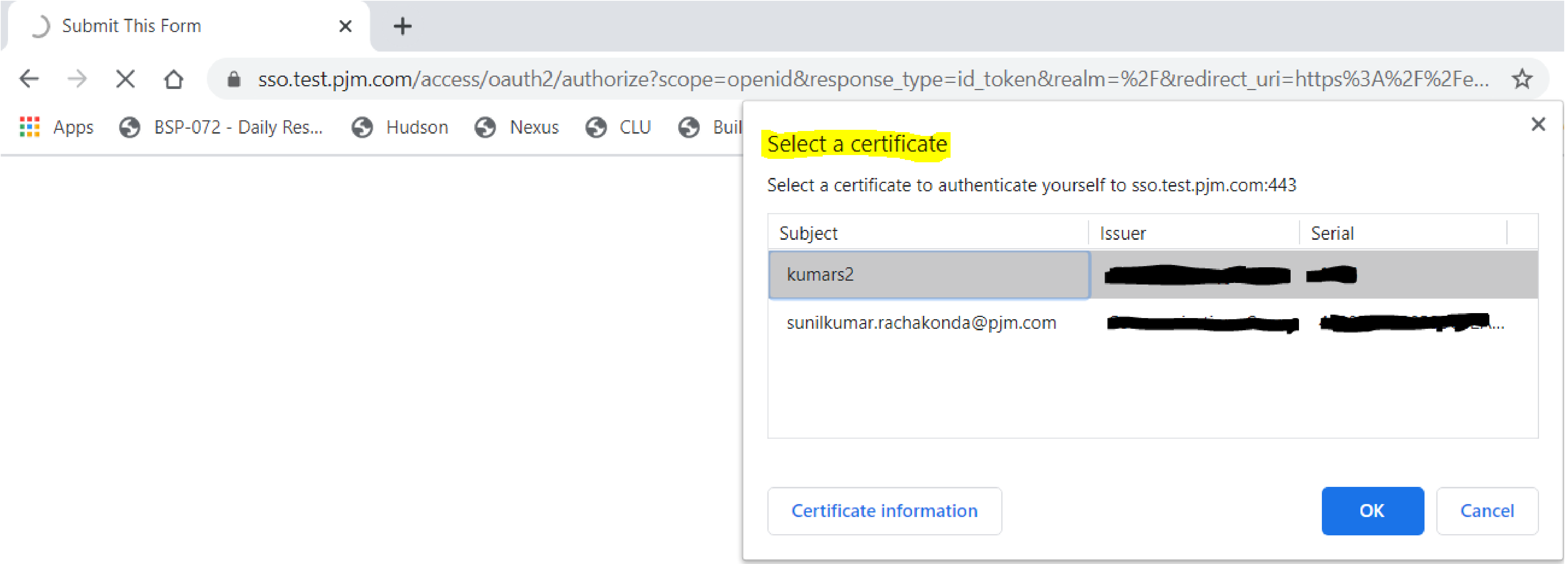
- Uploading Certificate
  - The User can upload the certificate or the CAM can associate certificates with user account from Account Manager PKI Tab



    - 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

ExSchedule and OASIS

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


Submit This Form
sso.test.pjm.com/access/oauth2/authorize?scope=openid&response_type=id_token&realm=%2F&redirect_uri=https%3A%2F%2Fe...
Apps
BSP-072 - Daily Res...
Hudson
Nexus
CLU
Buil

Select a certificate

Select a certificate to authenticate yourself to sso.test.pjm.com:443

Subject	Issuer	Serial
kumars2	[redacted]	[redacted]
sunilkumar.rachakonda@pjm.com	[redacted]	[redacted]

Certificate information
OK
Cancel

Browserless/API Changes

- 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’
```

PJM Command Line Interface (CLI)

- 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“
```

FAQs

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