



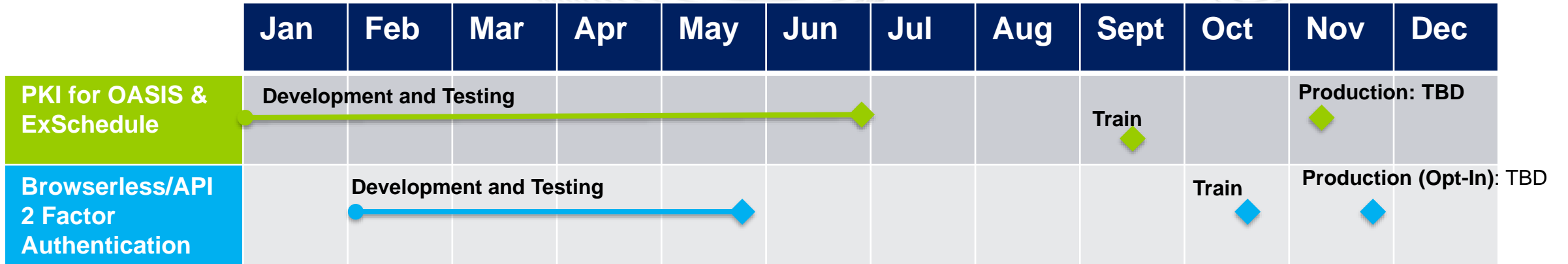
Tools Security Roadmap

As of July 15, 2020

- Updated Impact Details
- Updated Account Manager changes
- Updated Train & Production timelines

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>September 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>September 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





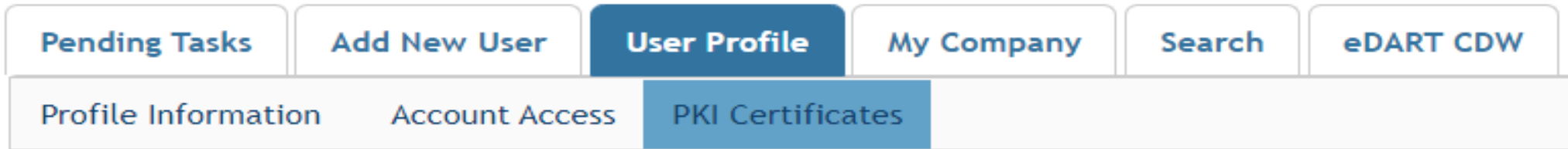
ExSchedule &
OASIS Public
Key Infrastructure
(PKI)

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: Sept
 - Production: Q4, 2020

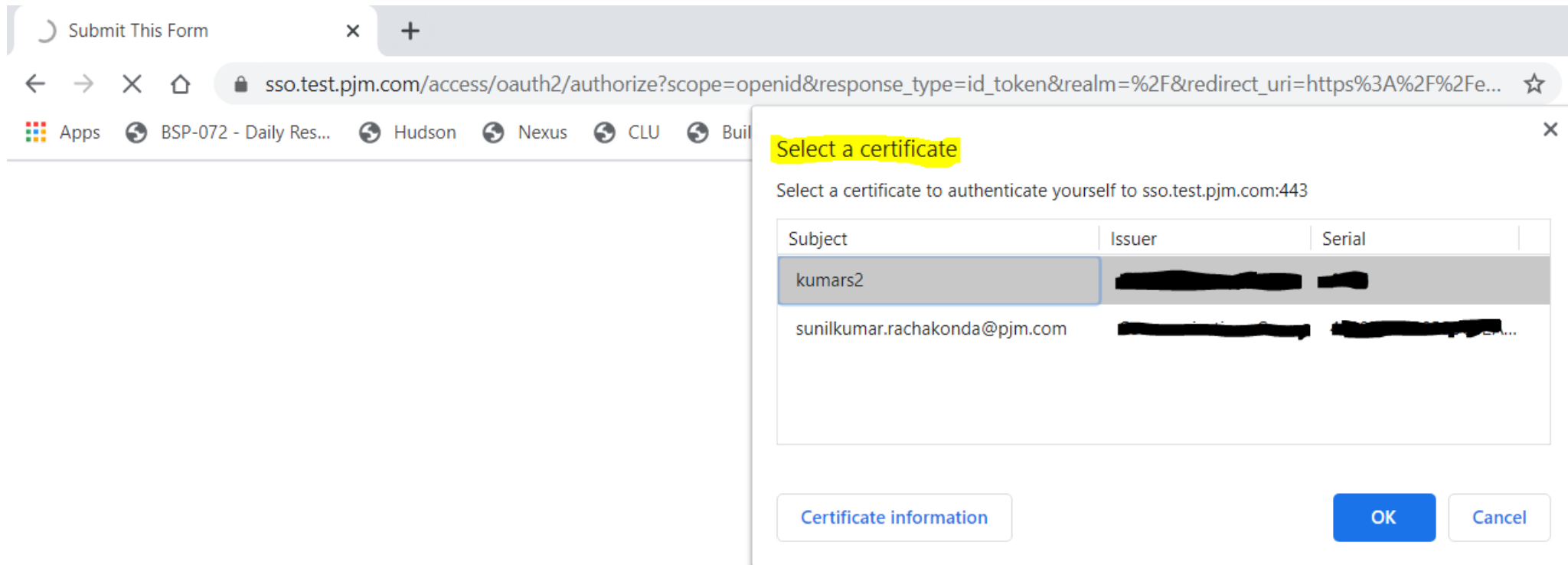
- Browserless/API 2 Factor Authentication
 - Leverage PKI solution
 - Scope
 - Included: All PJM Tools that are part of Single Sign On and have Browserless APIs
 - Excluded: ExSchedule and OASIS
 - When:
 - Optional in Q4, 2020
 - Mandatory in 2021

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



- CAM has to approve the upload
- Install the certificate on user's browser

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