



Tools Security Roadmap

As of May 18, 2021

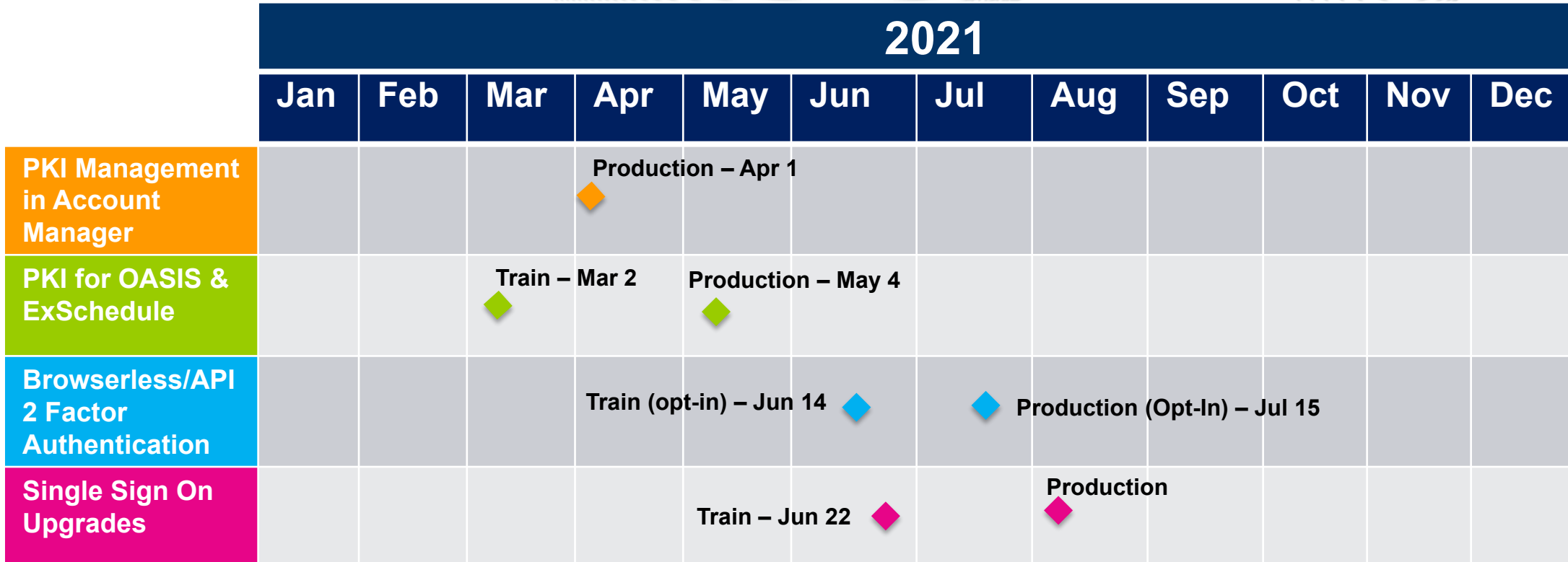
- Provided dates for PKI opt-in implementation
- Provided Train implementation date for Single Sign On (SSO) upgrade

Product - Action Required	Dates	Who May Be Affected
<p>Browser-less/API 2 Factor Authentication- Train (opt-in)</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) • Make sure 2-Way SSL Connections, Client Certificates & Connection Renegotiation are enabled at Firewall & Security devices for outgoing PJM SSO traffic 	<p>June 14 4 p.m. to 7 p.m.</p>	<ul style="list-style-type: none"> • Browser less users of Markets Gateway, InSchedule, Power Meter, FTR Center, Capacity Exchange, DR Hub



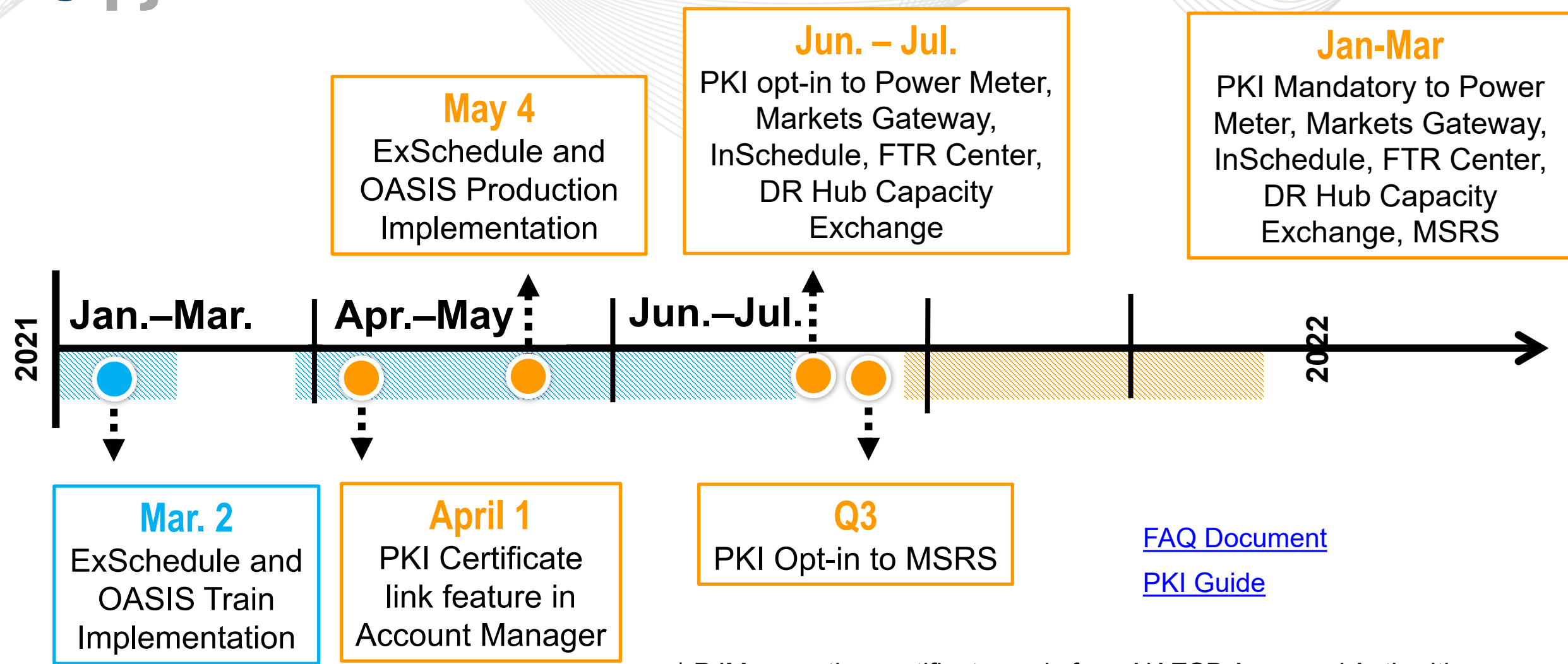
Product - Action Required	Dates	Who May Be Affected
<p>Single Sign on (SSO) System upgrade - Train</p> <ul style="list-style-type: none"> Any code parsing SSO Authentication response based on length will need to change. Use JSON parser or other methods 	<p>June 22 4 p.m. to 7 p.m.</p>	<ul style="list-style-type: none"> Any browserless code that depends on knowing the length of the token will need to change





Legend

- Start Date
- ◆ End Date

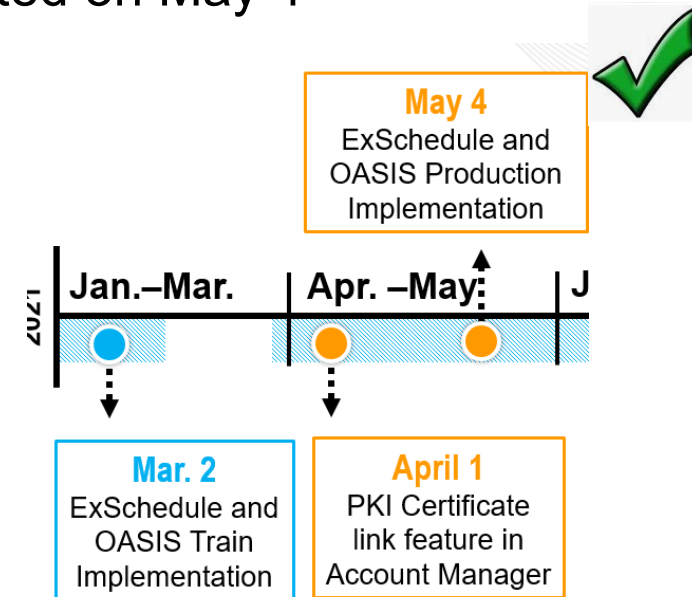


* PJM accepting certificates only from NAESB Approved Authorities

Lessons Learned from May PKI Implementation

- Certificate(s) must be installed on all machines used to access the tools
- User must select the correct certificate from browser pop-up
 - Ensure a match with what is uploaded to Account Manager
 - If an incorrect certificate is selected, the user must close all browser windows before retrying
- Browserless code must be updated on all servers/machines used to access the tools
- Step-by-step review of PKI Guide will help in smoother implementation

ExSchedule and OASIS successfully implemented on May 4




Browserless
API Two-Factor
Authentication

SSO Upgrades

- Leverage PKI solution
- Scope
 - Included: All PJM Tools that are part of Single Sign On and have Browserless APIs
 - Excluded: ExSchedule and OASIS
- Implemented In phases Optional then Mandatory
- Users can opt-in from Account Manager by requesting access to “Certificate Based Authentication Opt-In” role during the opt-in period
- For any reason users want to opt-out, they can work with their CAM to terminate access to the “Certificate Based Authentication Opt-In” role.

- Once opted in, the user is required to provide a valid PKI certificate for
 - Markets Gateway
 - InSchedule
 - Power Meter
 - FTR Center
 - Capacity Exchange
 - DR Hub
- When:
 - Train – June 14
 - Production – July 15
- MSRS opt-in will be implemented in Q3 2021
- The mandatory cut-over will take place in Q1 2022

 > Account Access > Request Access

1

Select Access


2

Review

Request Access

Accounts

PJM Interconnection [PJM]

 Certificate Based Authentication

Access

Certificate Based Authentication Opt-In



- Single Sign On (SSO) System upgrades
 - When:
 - Train: June 22
 - Production: August TBD
- Impacts
 - SSO Token length is changing with upgrade and not going to be a fixed value
 - Any code parsing SSO Authentication response based on length will need to change. Use JSON parser or other methods

```
{"tokenId": "yRQ9EqYG_1XpUXYE2C3yFDPPE9A.*AAJTSQAtDIA1NLABw2Y0N0ZjerZUh30GY4M2JjV29wc3BueWZweE09AAJT  
MQACMDc.*", "successUrl": "/access/console", "realm": "/"}
```

Presenter:

Sunil Kumar Rachakonda

SunilKumar.Rachakonda@pjm.com

SME:

Sunil Kumar Rachakonda

SunilKumar.Rachakonda@pjm.com

Tool Security Changes



Member Hotline

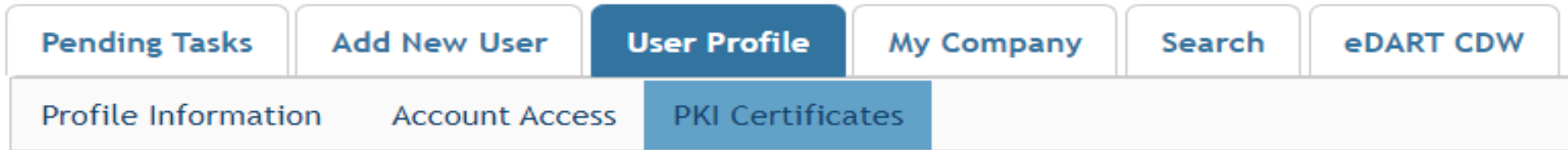
(610) 666 – 8980

(866) 400 – 8980

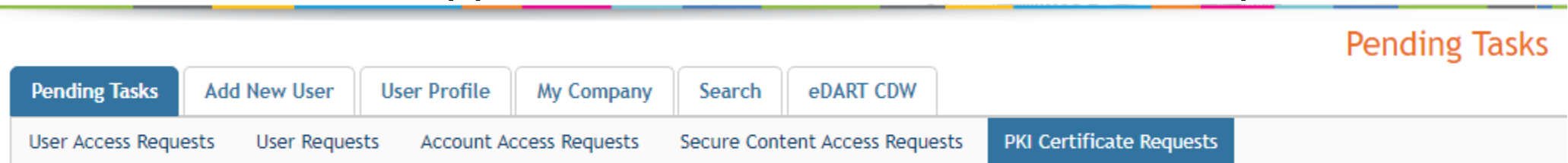
custsvc@pjm.com

Appendix

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

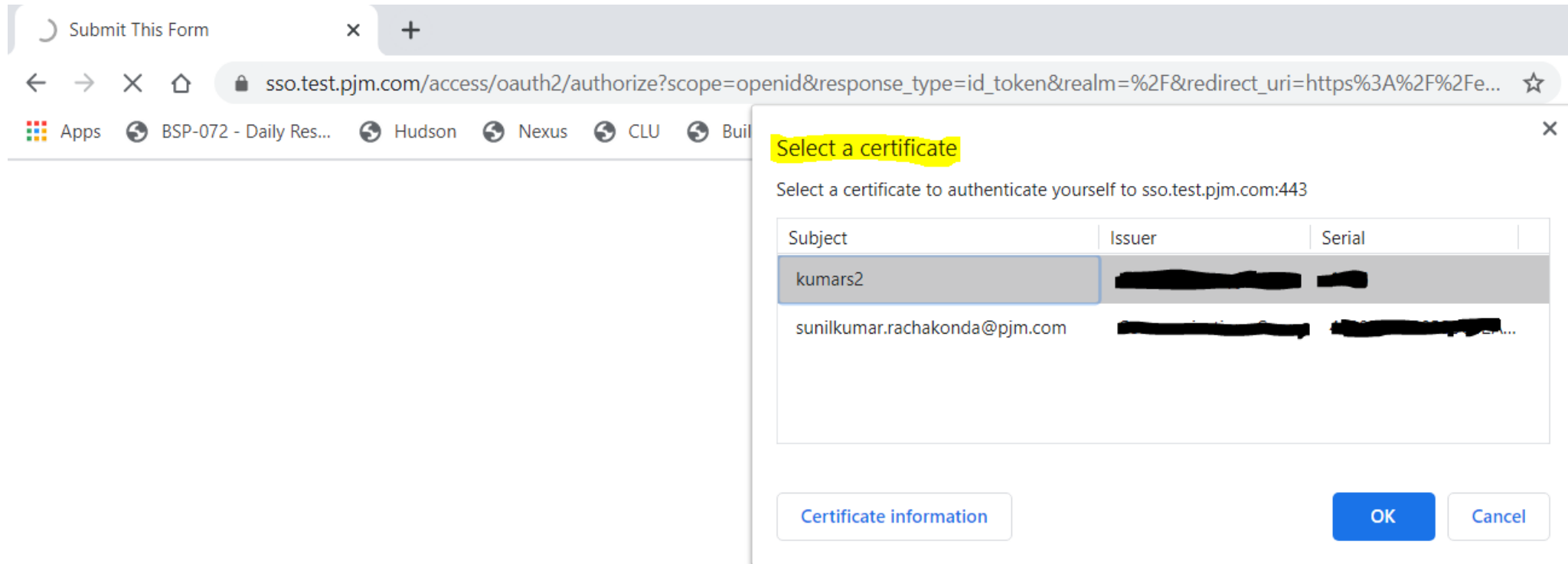


- The CAM has to approve the certificate after the user upload



- 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
- 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“`

- 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>

- 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>