Tools Security Roadmap

As of June 16, 2020
• Added new information for how to use Public Key Infrastructure (PKI) certificates in
  – Associating with a user account in Account Manager
  – Logging into ExSchedule and OASIS User Interface
  – Authenticating for browserless interaction
• Updated the PKI implementation timeline in Train
• Added information about the new PJM Command Line Interface which supports PKI
### Product - Action Required

<table>
<thead>
<tr>
<th>Account Manager Train</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Associate valid PKI certificates with user account in Account Manager</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Train Implementation for ExSchedule &amp; OASIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Obtain valid PKI certificates from approved Certificate Authorities</td>
</tr>
<tr>
<td>• Rewrite Browserless/API authentication code</td>
</tr>
<tr>
<td>• Use PJM provided command line interface (CLI)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dates</th>
<th>Who May Be Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 3</td>
<td>CAMs for users of ExSchedule and OASIS</td>
</tr>
<tr>
<td>August 10</td>
<td>Users of ExSchedule and OASIS</td>
</tr>
<tr>
<td></td>
<td>3&lt;sup&gt;rd&lt;/sup&gt; party Vendors for ExSchedule and OASIS</td>
</tr>
<tr>
<td></td>
<td>Developers of ExSchedule and OASIS Browserless/API code</td>
</tr>
<tr>
<td>Jan</td>
<td>Feb</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>PKI for OASIS &amp; ExSchedule</td>
<td>Development and Testing</td>
</tr>
<tr>
<td>Browserless/API 2 Factor Authentication</td>
<td>Development and Testing</td>
</tr>
</tbody>
</table>
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: Aug 10
    • Production: Q4, 2020
Background – Browser-less/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
  – When:
    • Optional in Q4, 2020
    • Mandatory in 2021
• Uploading Certificate
  – Associate certificates with user account from Account Manager PKI Tab
  – Install the certificate on user’s browser
ExSchedule and OASIS

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