PKI Implementation

Demand Response Subcommittee
December 9, 2021

PKI Implementation

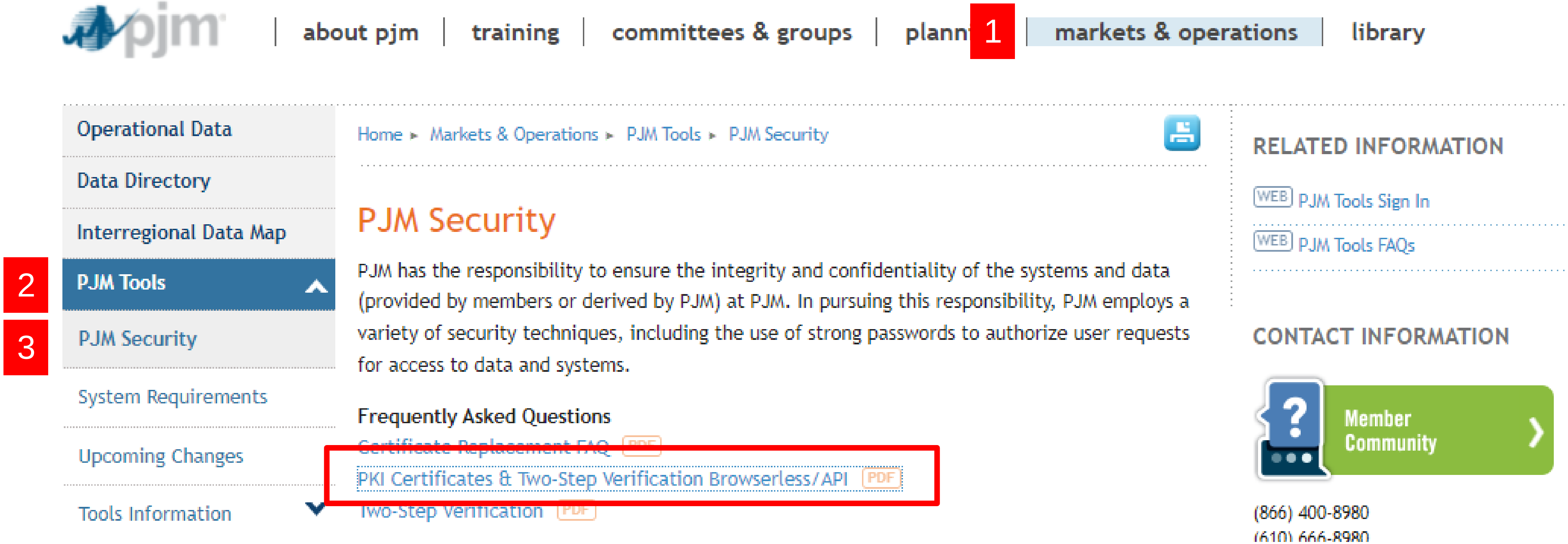
- Public Key Infrastructure (PKI)
  - Technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device and are safe to use. These documents are known as **certificates.**
  - Must purchase a certificate and upload it in Account Manager
- Only required for user ids that use Web Services or Browserless

Important Dates

- Implementation Dates
  - Train: January 11, 2022
  - Production: February 16, 2022

- If a userid for Web Services does not have a certificate by these dates, it will not be able to authenticate in DR Hub

Where to find more information



about pjm | training | committees & groups | plann 1 | markets & operations | library

Operational Data

Data Directory

Interregional Data Map

2 PJM Tools

3 PJM Security

System Requirements

Upcoming Changes

Tools Information

Home ▸ Markets & Operations ▸ PJM Tools ▸ PJM Security

PJM Security

PJM has the responsibility to ensure the integrity and confidentiality of the systems and data (provided by members or derived by PJM) at PJM. In pursuing this responsibility, PJM employs a variety of security techniques, including the use of strong passwords to authorize user requests for access to data and systems.

Frequently Asked Questions

Certificate Replacement FAQ PDF

PKI Certificates & Two-Step Verification Browserless/API PDF

Two-Step Verification PDF

RELATED INFORMATION

WEB PJM Tools Sign In

WEB PJM Tools FAQs

CONTACT INFORMATION

Member Community ›

(866) 400-8980

(610) 666-8980

https://pjm.com/markets-and-operations/etools/security