# Jetstream Guide
# DNP SCADA over Internet with TLS Security

PJM Interconnection

December 4, 2020

Manual and specification for data links between PJM and external parties, using the DNP3 protocol for communications, a Public Key Infrastructure based on TLS and X509 for security, and the public Internet for wide area networking.

## Revision History

| Version | Date | Modifications |
|---|---|---|
| 1.0.0.0 | 11/20/2013 – Ryan Nice | Initial release of User Guide. |
| 1.0.0.1 | 1/21/2014 – Ryan Nice | Fix miscellaneous editorial mistakes; font, chapter titles, etc. Edit section 4.4 to further clarify that dual-connected links are standard. |
| 1.0.0.2 | 8/19/2016 – Brian Orme | Reviewed Content for 2016. |
| 1.0.0.3 | 10/28/2017 – Brian Orme | Updated references to PowerMeter and reviewed content for 2017. |
| 1.0.0.4 | 12/4/2020 – Erkan Tuna | Updated language regarding TLS clients. Adjusted various formatting issues. |

## Table of Contents

# Chapter 1: Introduction

## 1.1 Document Description

This document describes the PJM method of transacting data with PJM members using the DNP3 data protocol over the public domain Internet secured with TLS. The specific PJM usage of each open technical standard employed is detailed to sufficient degree for planning and jointly establishing a data link between PJM and the member.

This document does not attempt to completely describe the DNP3 protocol, the TLS protocol, or the TCP/IP protocol. The appropriate authoritative technical documents for these protocols are referenced.

This document is not intended to explain PJM markets or operations. It will not help determine if a party is entitled to or in need of an Internet DNP data link with PJM, or the data content required for any given circumstance. PJM Manuals, PJM Client Managers, and the PJM Support Center should be engaged for help with those matters.

## 1.2 Intended Audience

Engineers, technicians, and technical officers charged with planning, establishing and maintaining an Internet DNP3 link with PJM. Basic functional understanding of DNP3, TCP/IP, X509 Certificates, TLS, PKI and electric power science is assumed.

## 1.3 Overview

For Jet Stream data links, PJM hosts two main functions, a DNP3 Master Station and a TLS Server. The remote site hosts a DNP3 Outstation and a TLS Client. The DNP3 Master Station and DNP3 Outstation engage in a conversation to exchange various data types bi-directionally to meet all operational and market data requirements. The TLS tunnel established by the TLS Server and TLS Client secures the conversation across the Internet.

Because DNP3 is a clear-text protocol with no inherent security mechanisms, TLS is used to provide data Confidentiality, party Authentication, and data Integrity. This is to ensure that the data is kept private, the parties are sure of whom they are communicating with, and no unauthorized third party can alter or malign the data en route without detection.

Essentially PJM and the site transact data with DNP3 exchanges. The DNP3 traffic is secured with TLS across the Internet, using both server and client certificates for mutual authentication.

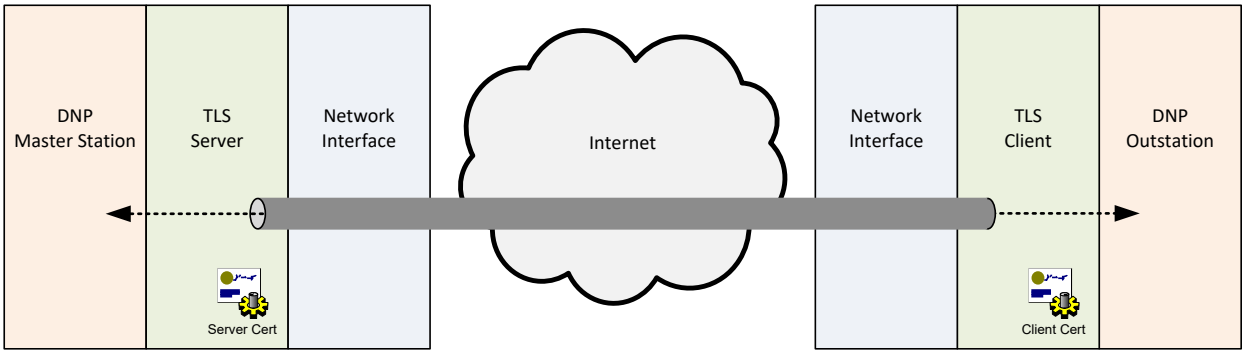


*Figure 1.*

## 1.4 Document Organization

This document is divided by the two major layers or components of a DNP3 Internet data link with PJM: the DNP3 protocol for communications and the TLS protocol for security. The Public Key Infrastructure is further broken down between the TLS protocol and the X509 certificate protocol.

## 1.5 Formatting

Binary data when presented literally will be written as octets in hexadecimal. Text font will change to Consolas (ex. `0123456789abcdef`) for further clarity.

# Chapter 2: DNP3

## 2.1 DNP3 Protocol

DNP3 stands for Distributed Network Protocol Version 3. The original standard was released by GE-Harris in 1993 and from inception was geared for North American utilities. Accordingly the protocol is used extensively in North America.

The protocol was designed to be very robust and efficient and has many features, like error checking and event reporting, to that end. Some features are more directly applicable in serial data connections (e.g. RS-485) but have been maintained even as the protocol made the jump to routable networks (e.g. TCP/IP).

The DNP Users Group is a nonprofit corporation dedicated to maintaining and promoting DNP3. Most recently DNP3 was adopted by IEEE as Std 1815-2012. This standard includes features of the latest iteration of DNP3 – Secure Authentication Version 5. PJM does not make use of DNP3 SAV5 at this time. Instead TLS is solely employed for security.

## 2.2 Basic Polling

PJM Master Stations request analog values and digital values from each remote station in real-time. Real-time in this context means the data is not time stamped but is assumed to represent the latest possible measured value. This type of data will be first used instantly in the PJM EMS and concurrently stored and time-stamped in a PJM historian. It is important that at each data transaction the Outstation replies with data values that represent actual physical conditions at that time. Accordingly any measurement, process, translation or calculation happening behind the Outstation must be done with sufficient speed that it does not introduce significant time delay in the data stream.

For Analog values PJM will issue requests once every 2 to 10 seconds, depending on the data requirements and site limitations.

For Digital values PJM will issue requests once every 2 to 10 seconds, depending on the data requirements and site limitations.

PJM requests revenue energy accumulator values in a frozen accumulated state. At any given time the Master Station requests accumulator data, the Outstation should reply with the value from the previous market hour. That replied value should stay the same (i.e. be frozen) over the entire hour. The value may either represent the hourly delta (the energy transacted over the prior hour) or a counter value (increments by the amount of energy transacted every hour).

For Accumulator values PJM will issue requests once every 10 minutes. The value taken immediately before half hour past each hour will be utilized for PJM market databases (e.g. PowerMeter Settlements).

For Setpoints values PJM will issue commands without a set periodic time. Commands will be sent immediately after two conditions are true: the setpoint value changes to be outside of the configured deadband, and the previous DNP command or request has been concluded. Additionally at minimum an integrity command will be sent once every minute if the setpoint value is constant.

## 2.3 Data Types

PJM commonly makes use of the following DNP3 objects and variations.

| | | |
|---|---|---|
| Analog Values | Object 30, Variation 2 | 16 bit integer with quality flags |
| Digital Values | Object 1, Variation 2 | Binary value with quality flags |
| Setpoint Values | Object 41, Variation 2 | 16-Bit Analog Output Block |
| Accumulator Values | Object 21, Variation 1 | 32-Bit Frozen Counter |

***Figure 2.***

These data types are considered a minimum for interoperability. In exceptional cases other objects and variations may be tried as needed at the discretion of both PJM and the connecting party.

## 2.4 Special Functions

The PJM Master will employ standard DNP3 data link function codes. For example RESET commands will be sent after a restart or recovery from a failure in order to prime and synchronize the two stations for communications. The TEST data link function code and REQUEST LINK STATUS messages are also often employed during the course of normal communications.

PJM transacts data almost entirely as 'static' data, where the DNP3 meaning of 'static' data is the most current value. DNP3 also has the provisions to transact event type data – historical, time-stamped, and limit or event driven data. PJM does not make regular use of event data over DNP3.

DNP3 has provisions for unsolicited messages where the outstation messages the master without a prompting request or command from the master. PJM does not make use of unsolicited messages. Unsolicited messages should be disabled at the outstation.

DNP3 has provisions for classes of data, whereby configurable subsets of event data can be grouped together into one or more of 3 different classes. PJM may make limited use of class features. For example during link recovery or reset a PJM master may request all class 0 data – which should return all static (real-time) data. Some outstations may incur processing or memory problems if too much event data is buffered. These outstations will usually use the IIN flags to indicate that class data is available and should be requested. PJM will optionally configure to respond to those IIN flags in order to help avoid outstation performance problems. However the event data transacted will not actually be processed or used by PJM in any meaningful way.

## 2.5 Exchange Examples

The following examples detail what the data payload of the TCP/IP packets might typically be during common DNP3 transactions between PJM and an outstation.

### 2.5.1 Analog Input Scan Example

PJM request for Analog Values 0 to 4:

**05 64 0d c4 12 00 00 00 33 43 c7 c3 01 1e 02 00 00 02 1b e2**

Where:

05 64 : The SYNC or start bytes.

0d : The length in bytes remaining in the frame. In this case 13 bytes.

c4 : The Control byte. In this case indicating station A to station B message, from the initiating station, and there is User Data that doesn't need confirmation.

12 00 : Destination Station Address. In this case slave or outstation address 18.

00 00 : Source Station Address. In this case master station address 0.

33 43 : CRC error checking.

c7 : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c3 : Application Control.

01 : Function Code. In this case indicating a read or request of specified objects from outstation.

1e 02 : Requesting Object 30, Variation 2, 16 bit Analog Input (integer) with status flag.

00 : Qualifier. In this case indicating a range scan with a start and stop field.

00 02 : Range, from data point 0 to data point 2, for a total of 3 data points.

1b e2 : CRC error checking.

Outstation response to request for Analog Values 0 to 4:

**05 64 18 44 00 00 12 00 4c 09 f8 c3 81 00 00 1e 02 00 00 02 01 80 00 01 09 00 01 07 01 00 00 47 e6**

Where:

05 64 : The SYNC or start bytes.

18 : The length in bytes remaining in the frame. In this case 24 bytes.

44 : The Control byte. In this case indicating station B to station A message, from the initiating station, and there is User Data that doesn't need confirmation.

00 00 : Destination Station Address. In this master station address 0.

12 00 : Source Station Address. In this case outstation address 18.

4c 09 : CRC error checking.

f8 : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c3 : Application Control.

81 : Function code. In this case indicating response to a request message.

00 00 : Internal Indication Bits. The outstation has nothing interesting here to indicate to the master station.

1e 02 : Giving Object 30, Variation 2, 16 bit Analog Input (integer) with status flag.

00 : Qualifier. In this case indicating a range scan with a start and stop field.

00 02 : Range, from data point 0 to data point 2, for a total of 3 data points.

01 80 00 : Analog Input data point 0, with value of 128, with online status.

01 09 00 : Analog Input data point 1, with value of 9, with online status.

01 07 : CRC error checking.

01 00 00 : Data point 2, with value of 0, with online status.

47 e6 : CRC error checking.

### 2.5.2 Binary Input Scan Example

PJM request for Digital value 0:

**05 64 0D c4 12 00 00 00 33 43 c1 c9 01 01 02 00 00 00 24 33**

Where:

05 64 : The SYNC or start bytes.

0d : The length in bytes remaining in the frame. In this case 13 bytes.

c4 : The Control byte. In this case indicating station A to station B message, from the initiating station, and there is User Data that doesn't need confirmation.

12 00 : Destination Station Address. In this case slave or outstation address 18.

00 00 : Source Station Address. In this case master station address 0.

33 43 : CRC error checking.

c1 : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c9 : Application Control.

01 : Function Code. In this case indicating a read or request of specified objects from outstation.

01 02 : Requesting Object 1, Variation 2, Binary Input (digital) with status flags.

00 : Qualifier. In this case indicating a range scan with a start and stop field.

00 00 : Range, from data point 0 to data point 0, for a total of 1 data point.

24 33 : CRC error checking.

Outstation response to request for Digital Value 0:

**05 64 10 44 00 00 12 00 90 93 EE C9 81 08 00 01 02 00 00 00 81 32 11**

Where:

05 64 : The SYNC or start bytes.

10 : The length in bytes remaining in the frame. In this case 16 bytes.

44 : The Control byte. In this case indicating station B to station A message, from the initiating station, and there is User Data that doesn't need confirmation.

00 00 : Destination Station Address. In this master station address 0.

12 00 : Source Station Address. In this case outstation address 18.

90 93 : CRC error checking.

ee : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c9 : Application Control.

81 : Function code. In this case indicating response to a request message.

08 00 : Internal Indication Bits. The outstation mentions it has Class 3 data available ready to be sent.

01 02 : Giving Object 1, Variation 2, Binary Input (digital) with status flags.

00 : Qualifier. In this case indicating a range scan with a start and stop field.

00 00 : Range, from data point 0 to data point 0, for a total of 1 data point.

81 : Binary Input (digital) data point 0, with a status of 1 (closed if breaker status) and on-line status.

32 11 : CRC error checking.

### 2.5.2 Accumulator Input Scan Example

PJM request for Accumulator values 0 to 3:

**05 64 0d c4 12 00 00 00 33 43 e1 c0 01 15 01 00 00 03 3f 23**

Where:

05 64 : The SYNC or start bytes.

0d : The length in bytes remaining in the frame. In this case 13 bytes.

c4 : The Control byte. In this case indicating station A to station B message, from the initiating station, and there is User Data that doesn't need confirmation.

12 00 : Destination Station Address. In this case slave or outstation address 18.

00 00 : Source Station Address. In this case master station address 0.

33 43 : CRC error checking.

e1 : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c0 : Application Control.

01 : Function Code. In this case indicating a read or request of specified objects from outstation.

15 01 : Requesting Object 21, Variation 1, 32 bit Frozen Counter.

00 : Qualifier. In this case indicating a range scan with a start and stop field.

00 03 : Range, from data point 0 to data point 3, for a total of 4 data points.

3f 23 : CRC error checking.

Outstation response to request for Accumulator values 0 to 3:

**05 64 23 44 00 00 12 00 83 89 e2 c0 81 08 00 15 01 00 00 03 01 c8 49 00 00 01 ed 7c 75 66 00 00 01 56 8a 00 00 01 e4 9d 00 00 1c 71**

Where:

`05 64` : The SYNC or start bytes.

`23` : The length in bytes remaining in the frame. In this case 35 bytes.

`44` : The Control byte. In this case indicating station B to station A message, from the initiating station, and there is User Data that doesn't need confirmation.

`00 00` : Destination Station Address. In this master station address 0.

`12 00` : Source Station Address. In this case outstation address 18.

`83 89` : CRC error checking.

`e2` : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

`c0` : Application Control.

`81` : Function code. In this case indicating response to a request message.

`08 00` : Internal Indication Bits. The outstation mentions it has Class 3 data available ready to be sent.

`15 01` : Giving Object 21, Variation 1, 32 bit Frozen Counter.

`00` : Qualifier. In this case indicating a range scan with a start and stop field.

`00 03` : Range, from data point 0 to data point 3, for a total of 4 data points.

`01 c8 49 00 00` : Frozen Counter (accumulator) data point 0, with a value of 18888 and on-line status.

`01 ed 7c 75 66 00 00` : Frozen Counter (accumulator) data point 1, with a value of 26229 and on-line status, including two CRC error checking bytes (inserted every 16 bytes data octets).

`01 56 8a 00 00` : Frozen Counter (accumulator) data point 2, with a value of 35414 and on-line status.

`01 e4 9d 00 00` : Frozen Counter (accumulator) data point 3, with a value of 40420 and on-line status.

`1c 71` : CRC error checking.

### 2.5.3 Analog Output Scan Example

PJM command analog output to outstation:

**`05 64 10 c4 42 00 00 00 ee f8 e2 c2 05 29 02 17 01 00 00 00 00 c8 bf`**

Where:

05 64 : The SYNC or start bytes.

10 : The length in bytes remaining in the frame. In this case 16 bytes.

c4 : The Control byte. In this case indicating station A to station B message, from the initiating station, and there is User Data that doesn't need confirmation.

42 00 : Destination Station Address. In this case slave or outstation address 66.

00 00 : Source Station Address. In this case master station address 0.

ee f8 : CRC error checking.

e2 : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

c2 : Application Control.

05 : Function Code. In this case indicating Direct Operate. Here Direct Operate means the output is both selected and set in one operation. This is in contrast to SBO, or Select Before Operate, functions where the value is selected then operated in two separate commands.

29 02 : Requesting Object 41, Variation 2, 16 bit Analog Output Block.

17 : Qualifier. In this case indicating an 8 bit single field count, in other words the next byte indicates the range.

01 : One point being sent.

00 : Point address is zero.

00 00 : Set value is zero.

00 : Point quality is online.

c8 bf : CRC error checking.

Outstation response to command for Analog Output 0:

**05 64 12 44 00 00 42 00 24 c1 f3 c2 81 0e 00 29 02 17 01 00 00 00 00 3f 61**

Where:

05 64 : The SYNC or start bytes.

12 : The length in bytes remaining in the frame. Does not include error checking bytes.

44 : The Control byte. In this case indicating station A to station B message, from the initiating station, and there is User Data that doesn't need confirmation.

`00 00` : Destination Station Address. In this case Master station 0.

`42 00` : Source Station Address. In this case Outstation address 66.

`24 c1` : CRC error checking.

`f3` : The Transport Header, in this case indicating it is both the first and final frame (the whole message is small enough to fit into one data link message).

`c2` : Application Control.

`81` : Function Code. In this case indicating Direct Operate. Here Direct Operate means the output is both selected and set in one operation. This is in contrast to SBO, or Select Before Operate, functions where the value is selected then operated in two separate commands.

`0e 00` : IIN

`29 02` : Requesting Object 41, Variation 2, 16 bit Analog Output Block.

`17` : Qualifier. In this case indicating an 8 bit single field count, in other words the next byte indicates the range.

`01 :` One point being sent.

`00` : Point address is zero.

`00 00` : Set value is zero.

`3f` : Point quality is online.

`61 bf` : CRC error checking.

## 2.6 DNP3 Outstation Address

PJM will associate a DNP3 address with the Distinguished Name of the site Certificate. DNP3 address will be provided by PJM to the site during the commissioning of the data link. It will be a permanent and unique value associated with that data link. Where a site hosts simultaneous connections to PJM AC1 and PJM AC2 control centers, the DNP3 address is the same for both data links. PJM may also select a specific Master Station address to accommodate site requirements.

# Chapter 3: Public Key Infrastructure

## 3.1 Certificate Authority

For the sake of efficiency and economy for all parties, PJM does not maintain and operate its own Certificate Authority (CA). OATI has been selected as the main CA in the PJM Internet DNP PKI. Other third party Certificate Authorities may be amended or removed from the trusted list in the future, as PJM continuously considers the best value and security for all members.

OATI conforms to NAESB WEQ-12 PKI standards and is an Authorized Certificate Authority, approved to issue digital certificates for use in NAESB EIR (webRegistry). The OATI webCARES program is widely accepted as a trustworthy service and product. However PJM cannot be held liable for the security, validity, or integrity of OATI webCARES digital certificates or other products. Each PJM member must make an independently informed and resolved decision about which Certificate Authorities are worthy of trust.

Both PJM and the remote site will possess a webCARES digital certificate signed and issued by OATI. Both PJM and the remote site will accept OATI as a trusted CA. It is the trust in OATI to only issue accurate and valid digital certificates that makes authentication between PJM and the site possible without any pre-shared secret keys, passwords or modules.

## 3.2 X509 Certificate

X509 v3 is a format standard for digital certificates as defined in IEC 5280. The X509 Certificate is a digital file describing the identity of the person or thing the Certificate was issued to, the technical features and uses of the Certificate, and the needed keys and signatures themselves. The OATI webCARES CA signs the Certificate. The signature is verifiable by any party who knows and trusts the CA. The signature represents assurance by the CA that they have verified the identity of the party described in the Certificate.

### 3.2.1 Example Outstation Certificate

Below is an example text output of a Certificate appropriate for PJM DNP3 SCADA use.

```
1  Certificate:
2      Data:
3          Version: 3 (0x2)
4          Serial Number:
5              12:f8:9f:da:00:00:00:00:79:cc
6          Signature Algorithm: sha1WithRSAEncryption
7          Issuer: C=US, ST=MN, L=Minneapolis,
           O=Open Access Technology International Inc, CN=OATI WebCARES Issuing CA
8          Validity
9              Not Before: Jan 24 19:38:02 2013 GMT
10             Not After : Jan 24 19:48:02 2015 GMT
11         Subject: emailAddress=johnsmith@xyzcorp.com, C=US, ST=PA, L=Norristown,
           O=XYZ Corp, OU=XYZ Energy, CN=Bear Creek Geothermal Energy Plant
12         Subject Public Key Info:
13             Public Key Algorithm: rsaEncryption
14             RSA Public Key: (2048 bit)
```

```
15                 Modulus (2048 bit):
16                     00:92:e5:... [continues for a total of 256 bytes]
17                 Exponent: 65537 (0x10001)
18         X509v3 extensions:
19             X509v3 Key Usage: critical
20                 Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
21             X509v3 Extended Key Usage:
22                 E-mail Protection, Code Signing, TLS Web Client Authentication
23             S/MIME Capabilities:
24         050...*.H..
25         ......0...*.H..
26         ......0...+....0
27         ..*.H..
28         ..
29             X509v3 Subject Key Identifier:
               4D:75:1C:B3:25:BF:B6:F6:DC:55:79:79:50:2C:99:E1:51:B3:09:79
30             X509v3 Authority Key Identifier:
               keyid:84:13:62:80:37:BE:A4:85:4D:6A:30:84:38:61:18:37:13:77:8F:5E
               DirName:/C=US/ST=MN/L=Minneapolis/O=Open Access Technology International Inc
               /CN=OATI WebCARES Root CA
               serial:12:9E:DB:CF:00:00:00:00:00:03
35
36             X509v3 CRL Distribution Points:
37                 URI:http://certs.oaticerts.com/repository/OATIIA2.crl
38                 URI:http://certs.oati.net/repository/OATIIA2.crl
39
40             Authority Information Access:
41                 CA Issuers - URI:http://certs.oaticerts.com/repository/OATIIA2.crt
42                 CA Issuers - URI:http://certs.oati.net/repository/OATIIA2.crt
43
44             Netscape Revocation Url:
45                 https://www.oaticerts.com/repository/nsrev_OATIIA2.asp?
46             2.5.29.7:
47                 0..
48
49     Signature Algorithm: sha1WithRSAEncryption
50         4d:c2:2e:… [ continues for a total of 256 bytes]
```

***Figure 3.***

Line 3: Certificate version. Must be version 3 (value 2).

Line 4: Serial number. Assigned by the CA. Is unique among all Certificates issued by a given CA.

Line 6: Signature algorithm. The Algorithm used by the CA to sign the certificate. In this case the content of the certificate is hashed with the SHA-1 cryptographic hash function then signed with the CA RSA private key. By using the CA public key to decrypt the signature and verifying the result matches the hash of the certificate, any party can trust the CA, who alone has the private key, did sign the certificate.

Line 7: Issuer. Describes the CA. In this case the location is in the US, Minnesota, Minneapolis, the organization is Open Access Technology International Inc, and the common name is OATI WebCARES Issuing CA.

Line 8 – 10: Validity. Describes the start date and end date of the certificate. After the certificate expires (or before the certificate starts) it will be rejected by the PJM server, extinguishing communications.

Line 11: Subject. Describes the identity of the person or thing the CA issued the certificate for. This will describe the company, control center, or particular asset that the data link with PJM is associated with.

Line 12 – 17: The Subject Public Key. The certificate owner may share this 256 byte key unsecured. Only the certificate owner will have the related Private Key, and therefore be the only party able to decrypt anything encrypted with the Public Key. The public and private keys are related by the RSA algorithm.

Line 18 – 22: Extensions. The Key Usage extension is a bit string that defines how a certificate can be used. The extensions are marked 'critical', meaning only identified uses are should be allowed. The uses allowed include:

- Digital Signature: digital signing of objects to prove the originator of message to recipient.
- Non Repudiation: indicates that certificate is sufficiently made such that the certificate owner could not deny actions taken with the certificate given reasonable scrutiny.
- Key Encipherment: the encrypting of symmetric keys with public keys. The certificate public/private key pair is used to securely share symmetric or session key. So the certificate key is used for secure communications and symmetric keys are used for bulk data transfer (DNP communications) for increased speed and processing efficiency.

The Extended Key Usage is a sequence of object identifiers that further defines which uses of the certificate are permissible. Note that it is not marked critical so these extended usages are only to indicate the intended purpose of the key.

- TLS Web Server Authentication: The Certificate can be used by a server to authenticate itself via TLS. The PJM TLS Server in the Internet DNP infrastructure will have this usage on its certificate.
- TLS Web Client Authentication: The Certificate can be used by a client to authenticate itself via TLS. The remote station will have this usage on its certificate.

Lines 23 – 28: Secure email. S/MIME is a standard for secure email applications and does not apply directly to this PJM application

Line 29 – 30: Subject Key Identifier. An extension to help identify certificates that contain a particular public key.

Line 36 - 38: CRL distribution. Identifies where the latest source copy of the Certificate Revocation List can be found.

Line 40-42: Authority information distribution. Identifies where the authority certificates can be found, in this case for both the root certificate and the issuing authority certificate. These are the certificates that should be added to the device or application list of trusted authorities.

### 3.2.2 Certificate and Identity

Some users will already possess an OATI webCARES digital certificate that is suitable for use in the Jet Stream System PKI. Some user organizations will already have an OATI Security Officer capable of immediately issuing a new OATI webCARES digital certificate for use in Jet Stream System PKI. Some trusted third-party vendors may act as a Security Officer, vouching for and procuring a certificate for a PJM member on their behalf, as a service. All users will ultimately have choices about many Certificate parameters.

The most common scenario will be that the Certificate identification parameters associate the Certificate with the site, asset or location most closely associated with that DNP3 Outstation. Ideally the Subject of the Certificate should logically and obviously identify the data link as specifically as possible without restricting its planned usage. For example, do not identify the Certificate as being for 'Bear Creek Generator Set Unit 1' if there are plans to also build Unit 2 and 3 at the site. Conversely do not identify the Certificate as being for 'Generator Set Unit 1'. Ultimately the acting Security Officer will decide how to name the certificate and will provide PJM with this information. PJM will then issue a unique DNP3 Outstation address and Master Station address that will be permanently associated with the Distinguished Name of the site public Certificate.

## 3.3 TLS

PJM will host a TLS Server which the remote site will connect and authenticate to. TLS is a protocol maintained by the IETF. The primary goal of TLS is to provide privacy and integrity between two communicating applications, in this case two DNP3 stations.

TLS is composed of two layers: the TLS Handshake Protocol and the TLS Record Protocol. The Handshake allows the server and client to authenticate each other and negotiate the algorithm and keys to be used, before the first application (DNP3) data is sent. The Record keeps the connection private by using the algorithm and keys (agreed upon during the Handshake) to encrypt the application data. It also includes some message integrity features that are redundant or complimentary with similar data integrity features in the DNP3 or TCP layers.

A further explanation is that the goal is to establish a secured communication channel with the desired party. The communication channel is a TCP/IP connection across the Internet. It is secured with symmetric key encryption, which is fast and efficient. Symmetric key encryption requires a shared secret (key) between the two communicating parties. The Handshake is what is used to prove the identity of parties to each other and then agree on those secrets. Identification is achieved by checking certificates, where each certificate associates an identity (a company or site name, etc.) with a public key. Each party has (and never shares) a private key associated with that public key. The public key allows each party to start private (encrypted) communications across an unsecure medium (the Internet) without any pre-shared keys or secrets or prior communications. This all hinges on the fact that each party trusts the certificate the other party is presenting, which is why OATI is the highly-trusted CA whom signs both the PJM and site certificate.

TLS is typically applied to and associated with web http applications. But it is equally well suited to secure any TCP/IP payload, including DNP3. Because it is a highly flexible protocol that can be applied to many different situations, interoperability demands detailed specification for each use.

PJM has adopted IEC 62351-3 for guidance and specification of both the TLS Server and Client. This part of the larger IEC 62351 technical specification intends to specify how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer. In this case the telecontrol protocol is DNP3 over TCP/IP.

### 3.3.1 IEC 62351-3

PJM's instantiation of IEC 62351-3 for TLS protocols includes the following requirements:

- TLS 1.0 (SSL 3.1), TLS 1.1, TLS 1.2 or higher shall be allowable. Proposal of any version prior to SSL 3.1 is not allowable.
- Any TLS cipher suite that specifies NULL for encryption may not be used. Examples deprecated suites include TLS_NULL_WITH_NULL_NULL or TLS_RSA_NULL_WITH_NULL_SHA.
- The TLS client must accept and handle periodic request from the TLS server to change the cipher sequence. This encryption key re-negotiation on established links further secures the link which is ideally long-lived and so may otherwise use the session keys for too long of a time period.
- Message Authentication Code (MAC) must and will be used.
- The client Certificate must be equal to or less than 8192 bytes in size and shall contain public keys that are at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.
- Certificate revocation shall be performed as specified in RFC 3280. The client and server will check the OATI Certificate Revocation List (CRL) at a periodicity not longer than once every 24 hours. The process of checking the CRL should not terminate the connection in any case. Revoked certificates will be denied connection at the server or client.
- Connections with expired Certificates will not be allowed.
- For key exchange, as a minimum, both RSA and Diffie-Hellman must be supported, with a maximum key size of at least 1024 bits.
- PJM will provide the TCP port number through which to exchange the TLS-secured DNP3 traffic during commissioning.

PJM requirements beyond or more detailed than IEC 62351-3 for TLS includes:

- The TLS client must support 'high' or 'strong' cipher suites. This requires key lengths larger than 128 bits. All cipher suites using AES-128 and AES-256 must be supported.

# Chapter 4: Architecture

## 4.1 PJM Control Center Redundancy

PJM operates two redundant active control centers. Each control center is physically and electronically completely separate providing a high degree of overall reliability. Both control centers fully support Internet DNP data links. PJM offers the option for one remote site to simultaneously connect to both PJM control centers.

The two PJM control centers are kept in sync, meaning that data at each site is compared in real-time and the best value is used at both sites. As a result dual-connecting an Internet DNP3 link provides redundancy. This redundancy extends to both incoming and outgoing data.

A typical non-dual-connected link would connect to one PJM control center at a time. PJM could at its option using networking technology move the server between control centers without intervention or interruption to the connections, but those cutover operations have no impact on site design or considerations.

A typical Jet Stream link will be redundant. The site will connect to and exchange DNP messages with both PJM control center, simultaneously and asynchronously.

## 4.2 Redundant Data Handling

For output data from PJM to the site, the output values from both control centers will be similar or identical at any given time. The two DNP Master Stations are operated uncoordinated. The remote site control system will have two streams of data to choose from. An acceptable scheme is to use the most recent received value, with no further coordination or comparisons between the two data streams. If either data stream slows or fails, the latest value will continue to be valid as the best data. PJM will maintain the data value consistency between the two data streams to prevent the latest value from bouncing between two disparate values every scan. For the site operators this is the main advantage of dual-connecting – higher reliability of PJM control signals, which can increase availability and participation in PJM markets.

For input data from site to PJM, the input values to both control centers must be of the same or similar values. The DNP Outstation or Outstations will be polled from the two DNP Master Stations in an uncoordinated operation. In all cases the most recent request from PJM should be met with the most recent measured value.

Sites that are dual-connected in particular need to carefully design the sequence of events for the local data quality flags. If one of the data streams serves PJM with inaccurate data values, PJM will automatically use the better data stream, if the bad data stream correctly sets quality flags indicating a compromised state. In DNP3 quality flags are present in both the IIN bits, which are internal indicators for the outstation, and the quality flag packed byte for individual data points. These flags should be fully employed to reflect actual site conditions and therefore ensure that data redundancy is actually increased for PJM and the member. If one data stream serves inaccurate data values but indicates good quality data with all flags and the data stream itself is healthy, then it is possible that PJM systems will use the incorrect data stream. Commonly data quality information can be lost between protocol translations and other data hops between devices, so particular attention should be paid to the interface between all measurement devices and the RTU.

## 4.3 Redundancy Depth and Design

Redundancy can be designed to many different depths. The site operator should weigh the cost to benefit of all design possibilities.

The common elements are that two separate PJM TLS servers will each receive a site client TCP/IP socket connection from the site over the Internet. Each connection will use the same Client Certificate. Each connection will resolve into a DNP session. The DNP data mapping and DNP Outstation address between the two separate DNP sessions will be identical.

All other elements of design are up to the asset owner. For example a design focusing on very high reliability may have two separate Internet Service Providers, two separate TLS Client devices, and two separate DNP Outstation devices with separate power supplies.

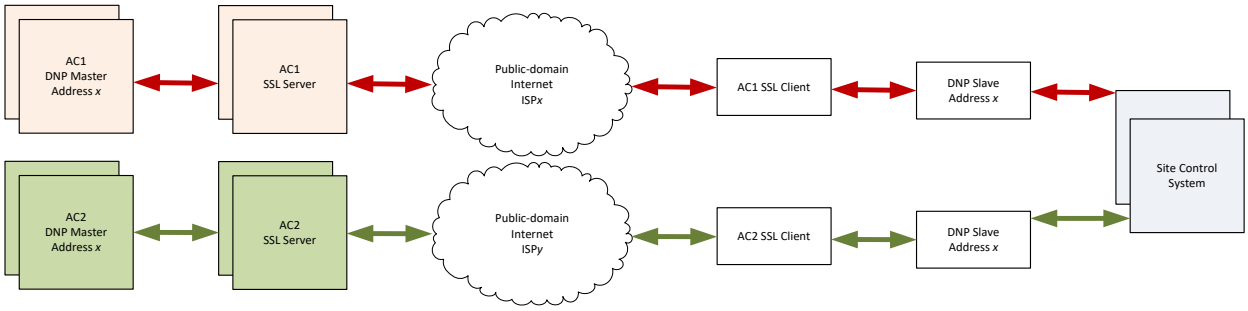


*Figure 4. Example High-reliability Dual-connected Architecture*

Alternately simplified designs could use the same TLS Client device to make both connections, and in some cases use the same Outstation instance to handle both data streams simultaneously. Connecting parties must balance cost and complexity against reliability goals when designing the system architecture.

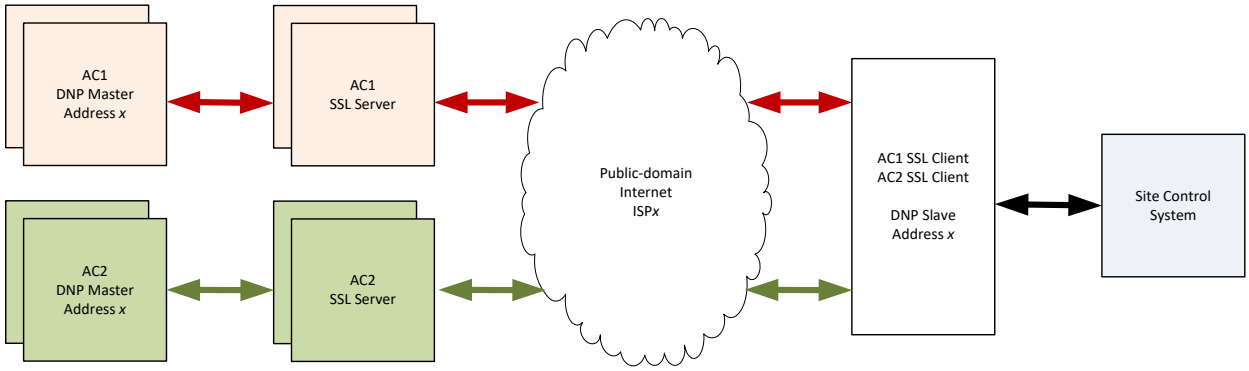


*Figure 5. Example Simple Dual-connected Architecture*

A site should review and coordinate the intended redundancy with PJM as early as possible in the interconnection process.

## 4.4 Single Connection Sites

It is possible for a site to have only one connection to PJM. This is particularly an option where the site does not receive any control signals from PJM, does not rely on PJM to auto-populate PowerMeter with accumulator values, does not represent a significant amount of capacity (approximately 10 MW) and is not located in an area prone to unique transmission constraints.

Sites with a single connection will by default connect to the PJM AC1 control center. However the site must maintain technical support to manually redirect the connection to the PJM AC2 control center in the case of a significant site failure. The site Security Contact or Telemetry Contact should be able to initiate the change quickly in an emergency event.

This design option will be deployed only under special conditions or constraints. Other than simplicity of design, there are no significant advantages to a single-connected site over a dual-connected site.

### 4.4 Data Latency Considerations

Some PJM markets incentivize better asset performance. This usually means quicker and more accurate asset response to a dynamic setpoint. Several aspects of the total data chain may cause either actual late asset response or perceived late asset response if not designed with proper consideration.

PJM will process and send the setpoint over the Internet in a timely manner which will not negatively impact the performance of an asset. In other words, PJM will not send a data point later than the asset is expected to respond. The PJM DNP master station will send data as quickly as it is processed every time the setpoint computes to a new value. However, once each setpoint value is sent, PJM does not account for its timely delivery. Receiving a setpoint late will cause the asset to actually respond late.

PJM will send requests for data, including data points associated with asset performance, for example MW and CREG. The PJM DNP master station will poll the outstation for data on a periodic basis, usually 2 seconds. This scan rate and corresponding compression settings in the PJM data historian are chosen for the required level of granularity to correctly assess the asset performance. However, if the response data values are late it will give the appearance of late asset response. This could be due to the response being late in transit back to PJM or the data source (meter or transducer) lagging behind the latest real measured value at the site.

If the intermediary network is slow, the additional latency will cause the asset to respond late, which may impact performance scores. This is rarely the case. Most Internet Service Providers are providing latencies between a site and PJM below 600 ms, which will not have a substantial impact on actual or perceived asset performance. DNP3 is very low bandwidth and will rarely challenge throughput capability on the connecting network.

Much more commonly significant latency in both setpoint and requested data is often incurred when multiple data hops between protocols and devices happen at the site. It is advantageous for the PJM master station to send setpoints directly to the asset-controlling device and for the PJM master station to receive requested data directly from the measuring device. Often this is not technically feasible, and an aggregating or intermediary device, like an RTU or gateway, connects to PJM, the asset-controlling device and the measuring devices. If not designed correctly the additional data hops can introduce latency.

This is because an intermediary device usually has an intermediary memory stack where input and output values are captured and buffered between site connections and the PJM connection. For example even if the PJM setpoint is being received at the site less than one second after it is sent, if an intermediary database is holding the value for several seconds before the actual asset-controlling device receives it, then actual asset response will suffer. Likewise, if the intermediary database is several seconds behind the actual measurement values, then perceived response will suffer.

Where intermediary databases are required, these negative effects can be counteracted by designing the site internal data links to update as quickly as possible. This may involve increasing scan rates, scanning by exception or event, using faster baud rates or processors, or removing unnecessary intermediary data hops completely. This is all a part of good site architecture and should be considered as early in the design process as possible.

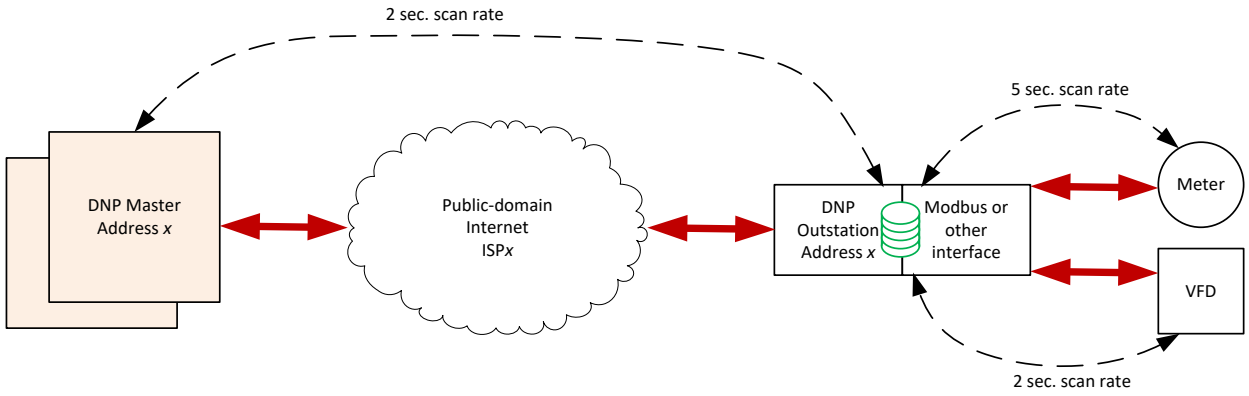


***Figure 6. Example of latency inducing architecture***

In Figure 5, the megawatt values from the meter would be up to 6 seconds late to PJM even given ideal network and processing speed. A regulation setpoint from PJM to the site could be received as much as 2 seconds late by the Variable Frequency Drive. The exact amount would be random based on the relation between the PJM scan and VFD scan start times, which are usually uncoordinated. In this case, the effect could be negated by forcing a scan to the VFD based not on a 2 second rate but the event of a new value from PJM.

# Chapter 5: General Security Requirements

By participating in the system described in this document, a relationship of trust is presumed between PJM and the connecting party. This trust is expressed both digitally at various technical layers and in cooperative designs and operations. Poor operational or security practices at any point of a data link can compromise the total security of the system for all parties involved. Therefore basic minimum thresholds for good practices are tacitly agreed to by connecting to PJM.

These guidelines expressed in this document are in general terms to allow for individual interpretation of and adherence to governing rules such as NERC/CIP. It is not the intention of PJM to interpret third party governing documents for connecting parties or dictate detailed security policy. It is the intention of PJM to publish useful security and operational guidelines for this system that also serves to detail PJM's minimum expectations. PJM reserves the right to disallow connection from a party if that connection is deemed a threat to the security or reliability of PJM systems.

## 5.1 Security Contact

PJM requires a contact be identified whom will represent the Member in technical security matters. The contact will often be the same person who acts as the OATI webCARES security officer and has direct operational responsibility for related telemetry and IT infrastructure.

Responsibilities of the Security Contact include:

- Procurement of the site certificate
- Secure transfer of certificate to devices
- Safe storage of certificate
- Certificate renewal, schedule and execution
- Understanding of other site security mechanisms (i.e. firewalls, intrusion detection devices, etc.)

## 5.2 Certificate Security

Protecting the private key of a Certificate is a critical factor in maintaining security. Failure to protect a Certificate private key could permit an attacker to impersonate the owner of the Certificate or decrypt information encrypted with the Certificate's public key.

The minimum amount of access to and exposure of the private key should be maintained. Turnover or reorganization of critical personnel with access to the private key should be considered cause to revoke and renew the Certificate.

## 5.3 Basic Network Controls

The remote site TLS client will be making the TCP/IP connection to the PJM TLS server. This starts with the creation of a TCP/IP socket and proceeds with the TLS handshake to complete the secured tunnel for DNP3 communications.

Because PJM has engineered the overall system so that remote sites are connection-making clients, no devices have to be in a TCP/IP LISTEN state. Accordingly no TCP ports have to be open from the Internet to any device in the remote site network in order to complete the connection to PJM. It is recommended that firewall rules between the Internet and internal networks are configured accordingly, with only site outbound connections enabled for the TLS Client device.

The actual instance of the DNP3 outstation may or may not be integrated into the same product as the TLS Client. When integrated into the same product the clear text DNP3 traffic is contained within that computing device. If the TLS Client and the DNP3 outstation are two separate products there will usually be a data link (e.g. a network TCP/IP or serial connection) between the two. This data link will usually carry the DNP3 traffic in clear text, unencrypted and unprotected. Therefore it is important in particular to secure the entirety of that portion of the data link within a protected network area.

## 5.4 Security Practices

For any device or software product that comes with a default username and password for any level of user or administration access, the username and password should be changed to something complex and unique. The minimum amount of access to and exposure of the user name should be maintained. Turnover or reorganization of critical personnel with access to the user name and password should be considered cause to change it. An example of a device username and password is an SSH session to a maintenance menu for a hardened gateway device.

It is recommended that any gateway devices be placed within the site electronic and physical security perimeter, as ESP and PSP is commonly defined by NERC/CIP standards. Even if the device is placed outside of the strictly defined ESP and PSP, it is recommended that some instance of a DMZ network be used and physical access restricted.

Some gateway devices can be configured to perform a variety of protocol and logical functions. Most likely there will be a DNP3 or Modbus data stream in clear text between the gateway and some other data source, like a meter or control system or another RTU. Because these data streams are relatively predictable in structure and context, it is possible to monitor the data accordingly. For example, if the gateway needs to collect all PJM data from a single Modbus RTU, the Director should not be attempting any other network connections, and detection of such connections should throw critical alarms. It is recommended that all gateway devices and software be restricted to the activities it was designed for and be monitored for anomalous or suspicious behaviors.

# Chapter 6: General Operational Requirements

## 6.1 Telemetry Contact

PJM requires a contact be identified whom will represent the Member in operational matters. The contact may be the same person who acts as a Security Contact and has direct operational responsibility for related telemetry and site operations.

Responsibilities of the Security Contact include:

- Maintaining the accuracy, scaling, and timeliness of data
- Verifying actual plant operations and conditions
- Technical and troubleshooting response
- Communication of telemetry outages and maintenance to PJM

## 6.2 Operational Requirements

Control center and data exchanges requirements are detailed in PJM Manual 01 (M-1). Manual 14D (M-14D) focuses on generator responsibilities and related market and operational requirements. Other formal operational or telemetry requirements may apply as expressed in other PJM Manuals.

# Chapter 7: New Link Commissioning Process

Some important preconditions to establishing and operating an Internet DNP3 data link with PJM are PJM Membership or formal permission from a PJM Member to act as a data transaction substitute, active and ongoing adherence to PJM Manuals, and established operational or market justification for the data link.

## 7.1 Designing and Testing a Coherent Architecture

For many projects, beginning participation in PJM markets requires establishing a DNP3 data link as one of many tasks that must be completed. Though the data link is often a minor task in respect to a large complex project, it is often critical to beginning participation in markets.

Initial design of the site architecture should consider the actual data requirements of the project as early as possible. This is important in two respects. The various data paths must include routes for all required measurement devices. And the various data paths must include routes for all required control devices.

Measurement devices are typically revenue meters, power meters, transducers, breaker status relays, similar substation or field devices, or an intermediary aggregating device like an RTU or PLC. For every measurement value required by PJM, the data path from that measurement device to the DNP Outstation should be accounted for.

Control devices are typically a control system, or alternately, a human operator. Many positions in PJM markets require control data, or data flow from PJM to the site. For every control value sent by PJM and required for the site, the data path from the site DNP Outstation to the controlling device or personnel should be accounted for.

If dual-connecting, as described in Chapter 4, the intended redundancy design should be coordinated with PJM engineers.

Visibility into the site ends at the DNP3 Outstation for PJM. Maintenance and troubleshooting between the Outstation and site measurement and control devices is the responsibility of the PJM member. PJM will facilitate troubleshooting as possible.

## 7.2 Procuring a Certificate

The PJM DNP3 PKI includes OATI as the Certificate Authority. Therefore the site certificate must be obtained by the site (directly or through a third-party) from OATI through the OATI webCARES System. The webCARES system can be accessed by an OATI Security Officer. The Security Officer essentially acts as the PKI Registration Authority. See Section 3.2 for a detailed specification of the client Certificate.

Through OATI webCARES System, a Security Officer will issue the Certificate. There are several ways a site could procure a Certificate for the data link:

- use an existing OATI Certificate, appropriately formed for the data link
- use an existing OATI Security Officer to issue a new Certificate
- have a site person register with OATI as a new Security Officer to issue a new Certificate

- PJM maintains a listing of third-party service providers that may be able to act as the Security Officer and Registration Authority for the site. The services may include the ability to issue and renew Certificates and otherwise act as the OATI Security Officer for the site.

The client certificate is the 'EEC Type' in the webCARES interface.

The OATI webCARES system is located at www.oaticerts.com and the CAcertificate and CRL repository can be found at www.oaticerts.com/repository/.

A first time user walk through is located at https://www.oaticerts.com/repository/newuser/NewUserWelcome.htm

### 7.3 Procuring a TLS Client

PJM maintains a listing of certified TLS vendors that deploy TLS clients. These TLS clients have been jointly tested by PJM and the vendor for interoperation with the PJM TLS server. The list gives reasonable assurance that a product will interoperate with PJM, however the site must still perform due diligence regarding the specific project details and requirements that may impact the successful integration of any product. The TLS Client product may or may not include other functional blocks, like the DNP3 Outstation, protocol conversions, separate data processing similar to an RTU, etc. Note that PJM can only vouch for the operation of the TLS Client and connection to the DNP3 Outstation.

PJM may optionally allow custom, one-off, or personalized TLS Client software or devices to be employed. Acceptable instances would involve a technically mature member with sufficient technical resources to comprise and integrate their proposed solution without undue development or testing burdens being placed on PJM.

### 7.4 Procuring a DNP3 Outstation

The DNP3 Users Group maintains an online listing of conformance tested vendors and products. This list provides a valuable starting point if a preferred vendor is not found. Because DNP3 is a highly stable and ubiquitous data protocol within the electric utility industry PJM does not make specific recommendations. Any product claiming conformance testing success to DNP3 should be able to interoperate with PJM given the correct configuration. See Chapter 2 for details about PJM's standard DNP3 operations.

PJM may optionally allow custom, one-off, or personalized DNP3 outstation software or devices to be employed. Acceptable instances would involve a technically mature member with sufficient technical resources to comprise and integrate their proposed solution without undue development or testing burdens being placed on PJM.

### 7.5 Commissioning Process

The exact commissioning process will depend on the exact market or markets being entered and the context of the project.

In cases where the site asset is part of the PJM model of the grid with associated real-time data, the data must be verified between PJM operations and site operations. When possible this should be done in two phases: before energization or market entry and after energization and market entry.

Before energization or market entry the integrity of the data link and either preliminary or simulated values will be verified. Integrity and function of the data link should be confirmed as soon as possible to reduce risk to the project. Testing of data values before energization and market entry is often a prerequisite to making significant power flows.

When site operation includes nominal flow of test power, real-time telemetry will again be verified, confirming scaling and accuracy. Completion of this testing is often sufficient to then fully participate in the market. Further steps may be necessary for addition services – for example verification of revenue meter accumulators for auto-population into PowerMeter.

During this process members should work primarily through their PJM Interconnection Coordinator and PJM Client Manager. Personnel contacts for telemetry tasks will be provided.

Sensitive information may need to be passed between PJM and the site, including IP addresses, electric one-line drawings, DNP3 data maps, etc. This documentation should not be sent unsecured, for example plain email attachments. Instead application level encryption with password (ex. encrypted Microsoft Excel files) or secure file sharing methods (ex. sftp) should be used.

### 7.6 PJM and Site Information Exchanges

This section lists the common exchanges of information during a new link commissioning in roughly chronological order.

- Site to PJM: Intended market entries for assets (often during the Interconnection Process)
- PJM to Site: Required input and output data for support of PJM markets and operations.
- Site to PJM: Public Certificate.
- Site to PJM: DNP3 Data Map defining the DNP3 Object and Variation, and definition of each data point corresponding to the required input and output data.
- PJM to Site: DNP3 Outstation address.
- PJM to Site: Port numbers and IP addresses for the TLS Server.
- Site to PJM: Intended energization or market-entry date.

## Acronyms and Abbreviations

DNP3 – Distributed Network Protocol version 3

DNP3 SAV5 – Distributed Network Protocol version 3, Secure Authentication version 5

TLS – Transport Layer Security

SSL – Secure Socket Layer

PKI – Public Key Infrastructure

Cert – Certificate (X509)

CA – Certificate Authority

TCP/IP – Transmission Control Protocol / Internet Protocol

PLC – Programmable Logic Controller

RTU – Remote Terminal Unit

IETF- Internet Engineering Task Force

CRL- Certificate Revocation List

DN – Distinguished Name

## References

RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force. May 2008.

RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2. Internet Engineering Task Force. August 2008

RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1. Internet Engineering Task Force. April 2006

RFC 2246: The Transport Layer Security (TLS) Protocol Version 1.0. Internet Engineering Task Force. January 1999

RFC 793: Transmission Control Protocol. Internet Engineering Task Force. September 1981.

RFC 791: Internet Protocol. Internet Engineering Task Force. September 1981.

TS 62351-3: Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP. IEC. First edition 2007-06

P009-0PD.DL: DNP V3.00 – Data Link Layer. DNP Users Group. Document Version: 0.02. Last edit May 30/97.

1815-2012: IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3). 2012