Jetstream Certification and Testing

PJM Interconnection

10/28/2017

This page is intentionally left blank.

Introduction

Document Description

PJM maintains and publishes a list of certified devices, software packages or other products that have been tested and proven to properly interoperate with the PJM Jetstream system. The publication is intended to help end users find products with a high measure of convenience and assurance of functionality. Product certification requires conforming to this document of requirements and scheduling, executing and passing performance tests with PJM. This document defines both the technical requirements of the product and the testing and certification approach used before a product is recognized by PJM as certified.

Asset owners and operators may develop their own solutions independent of third party vendors. Non-commercial, non-public, or custom projects may be similarly supported but must likewise meet the minimum requirements and be sufficiently planned and supported as to not create an unusual integration or maintenance burden.

Intended Audience

Engineers, technicians, and technical personnel charged with developing new products and services that will interoperate with the PJM Jetstream system. Basic functional understanding of DNP3, TCP/IP, X509 Certificates, TLS, PKI and electric power science is assumed.

Overview

The PJM Jetstream system is for DNP3 communications between PJM and a remote site across the Internet. The Jetstream Guide is the primary document for overall description of the system and instructions for integration and operation. This document is targeted to parties developing products interoperable with the PJM Jetstream system. It further clarifies and amends the system described in the Jetstream Guide including additional technical requirements specific to a product interoperable with Jetstream. This document will also describe the Certification Process, whereby products are tested in a collaborative effort between PJM and the Developer.

For Internet DNP 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.

The total data path can be summarized as PJM EMS to PJM DNP3 Master Station to TLS Server to Internet to remote site TLS Client to remote site DNP3 Outstation to remote site Control System.

The interoperable product may be the TLS Client, the DNP3 Outstation, or both as substantiated in hardware, software, or a combination of both. The testing may be for one specific product or a family of similar products. Families of products that have the same source code and processing for the network, DNP3 and SSL/TLS layers may be tested as one product.

Individual variations or modules not related to the core TLS client and router or DNP3 outstation do not need to be separately tested.

The minimal instance of a product would be a TLS client that is capable of establishing the TLS tunnel with the public PJM servers and routing DNP3 traffic to an external instance of a DNP3 outstation. This would necessitate adherence to the Certificate Management and TLS Support requirements in this document. If a DNP3 outstation can be instanced in the product, then the DNP3 Outstation requirements must also be adhered to. In all cases, the General Requirements and Security Requirements must be adhered to.

General Requirements

The product shall be configurable and capable of supporting all operations, qualities and configurations described in the Jetstream Guide. The Product shall be compliant with all relevant standards and good practices typical for the class of hardware or software being developed.

The product shall accept certificates issued by OATI, use a client certificate to authenticate to PJM, check server certificates against an OATI CRL, and establish a TLS session. Two separate TLS sessions must be supported, one to each PJM control center. See the Jetstream Guide for a description of redundant operations. Each TLS session will be host to a DNP3 conversation. The Product shall provide consistent data to both PJM DNP3 master stations, accept setpoints or analog outputs from both PJM DNP3 master stations and be able to combine each source into one latest received data point (unless it is a routing or pass-through only device).

The Product shall be able to automatically recover from power outages, network outages and other temporary interruptions, and resume normal operations without human intervention.

Documentation

Documentation for the product must be freely available to all end users, detailing at minimum how to:

1. Install an X509 certificate for use to connect and authenticate with PJM using TLS
2. Create a Certificate Signing Request with a Private Key generated locally on the device, therefore allowing a signed certificate to be procured without ever having the private key outside of the device
3. Add Certificate Authorities to the trusted list
4. Manage Certificate Revocation List, including enabling options for automatic download of CRL files from remote repositories
5. Configure a TLS client
6. Configure a DNP3 outstation (if feature is available)
7. Route DNP data streams from PJM to other external targets (if feature is available)
8. How to make connections between the TLS client and DNP3 Outstation

Documentation must also explicitly describe:

1. The vendor's stated practice for security patches and updates to the product
2. Dependencies on common libraries or code distributions that are frequently updated (for example OpenSSL)

Documentation must be up to date with the latest product versions and features.

DNP3 Requirements

If the Product can substantiate a DNP3 Outstation, then Product needs to be a fully qualified DNP3 compliant device. DNP3 is defined by one of two public standards: either 1815-2010 - IEEE Standard for Electric Power Systems Communications -- Distributed Network Protocol (DNP3), or P009-0PD.DL – DNP Users Group DNP V3.00 DATA LINK LAYER. The Vendor is responsible for adherence to either of these standards. Use of libraries, source code or DNP3 drivers is allowable, but the vendor is responsible for the soundness and functionality of that code.

The Jetstream Guide describes normal PJM to site DNP3 operations. These common operations and data types will be specifically tested initially, and should be regression tested if any product changes or updates are deployed.

TLS Requirements

Cypher Suites

The product must support the following cipher suites:

OpenSSL Cipher Suites	
ADH-AES128-GCM-SHA256	ECDHE-ECDSA-AES256-SHA
ADH-AES128-SHA256	ECDHE-ECDSA-AES256-SHA384
ADH-AES256-GCM-SHA384	ECDHE-RSA-AES128-GCM-SHA256
ADH-AES256-SHA	ECDHE-RSA-AES128-SHA
ADH-AES256-SHA256	ECDHE-RSA-AES128-SHA256
AECDH-AES128-SHA	ECDHE-RSA-AES256-GCM-SHA384
AECDH-AES256-SHA	ECDHE-RSA-AES256-SHA
AES128-GCM-SHA256	ECDHE-RSA-AES256-SHA384
AES128-SHA	ECDH-RSA-AES256-GCM-SHA384
AES128-SHA256	ECDH-RSA-AES256-SHA
AES256-GCM-SHA384	ECDH-RSA-AES256-SHA384
AES256-SHA	PSK-AES128-CBC-SHA
AES256-SHA256	PSK-AES256-CBC-SHA
CAMELLIA128-SHA	SRP-AES-128-CBC-SHA
DHE-DSS-AES128-SHA	SRP-AES-256-CBC-SHA
ECDH-ECDSA-AES256-GCM-SHA384	SRP-DSS-AES-128-CBC-SHA
ECDH-ECDSA-AES256-SHA	SRP-DSS-AES-256-CBC-SHA
ECDHE-ECDSA-AES128-SHA256	SRP-RSA-AES-128-CBC-SHA
ECDHE-ECDSA-AES256-GCM-SHA384	SRP-RSA-AES-256-CBC-SHA

The PJM TLS Server may negotiate any subset of the listed cipher suites, so guaranteed interoperability demands all are supported. At any given point in time PJM may deprecate any of the cipher suites, in particular if a vulnerability specific to

that suite is found. Future cipher suites may be added but will be done so with overlapping use of prior listed suites as to allow for time for adaptation.

The PJM TLS Server will renegotiate the connection periodically. This is to make sure that session keys are not used for sufficient timespan or amounts of data that an attack on the connection is made possible. The renegotiation time cycle or byte cycle will be sufficient for security but intermittent enough to not materially impact DNP3 communications. The TLS Client must accept, handle and execute the renegotiation requests under all circumstances.

The TLS client must be able to support TLS versions 1.2, 1.1 and 1.0.

Certificate Management Requirements

The Product must allow the user to choose one or more trusted third parties or trusted Certificate Authorities. The application will then trust certificates signed by any of the trusted Certificate Authorities or Issuing Authorities.

The product must be able to support SHA1 or SHA2 hashes in X509 certificates.

The Product must also allow the user to configure additional authentication of the PJM connection. For example a parameter of the PJM server certificate, like the distinguished name.

The Product must allow the user to download one or more Certificate Revocation Lists. The Product will check the CRL at least every time a new connection is made. If the other party presents a certificate that has been revoked, the connection must terminate and alarm logging generated. The CRL should be checked for a signature by a trusted CA.

The Product will support CRL files with maximum file size of at least 2 megabytes.

By 11/2014 all Products must also allow a user to configure a public repository of a CRL. The Product will use the URL of the repository to automatically update the internal CRL file, based on a configurable time periodic automatic download.

The Product must be able to internally create a Certificate Signing Request and a public private key pair on the device or software instance. As such, the movement, copying or manipulation of the private key is not necessary for procuring a signed certificate. The CSR should be exportable for use to create the final client certificate.

The Product shall have a user interface that allows a privileged user to view the client certificate, trusted certificates, and the live connected server certificate – including the Distinguished Name values.

The memory location where the certificates and keys are held shall be protected, allowing the user to limit access by common means, such as password or group.

Networking and Dual-connecting

The Product shall be able to accept the PJM Jetstream server domain name or IP address, and port number, as connection parameters. All connections shall have a configurable socket timeout parameter, by which the socket is completely closed then attempted for re-establishment based on no data being received over the connection for a configurable amount of time.

The Product shall be able to simultaneously connect to two discrete PJM Jetstream servers. The connections will be independent and asynchronous. The two connections to two separate PJM TLS servers may present the same client certificate for authentication. Each connection will have a separate, independent, asynchronous DNP3 master station from the PJM TLS server side. Whether these master stations are routed to separate DNP3 outstation instances sharing a database, the same DNP3 outstation instance, or routed to external devices as clear-text DNP3, is a matter of design. The Product documentation and materials must explicitly describe what it is capable of in terms of any design or performance limitations, specifically in regards to supporting the PJM dual-connection architecture. This architecture is further described in the Jetstream Guide.

Security

The Product shall be free of static default user accounts, hidden login or maintenance ports, or any other methods of digital entry or manipulation not explicitly documented for the user.

The Product shall not use any operating system, library, source code or other digital technologies with known significant unresolvable security defects, vulnerabilities or stability problems.

The Product shall be maintained with patches, hotfixes or version updates as needed to maintain the security and integrity of the product as knowledge of threats and vulnerabilities evolves.

Testing and Certification

A real or simulated remote site will host a typical instance of the Product. A test time and specific test scope will be discussed and agreed upon. Testing will establish repeated success of all TLS and DNP3 operations described in this document and the Jetstream Guide. Testing will be sequentially as follows:

1. Product authentication to PJM servers
2. DNP3 transactions over a TLS session
3. Security checks for TLS two way assurance, protection of secrets keys, etc.
4. Dual-connection functionality, including providing data to PJM consistently across both DNP sessions and properly handling the same data SetPoint from two different PJM sources
5. Auto-recovery properties, including simulated interruptions, power failures and network failures
6. Burn-in and stability, including at least 7 days of stable uninterrupted operation under realistic production conditions