

DRI Project: DNP Secure Authentication

ISO New England Smart Grid Demand Resource Integration (DRI) Project

Wednesday, April 15, 2009

Purpose

The purpose of this document is to describe the use of DNP3 Secure Authentication (DNP3 SA) to enable secure communications between the ISO New England Communication Front End (CFE) and vendor RTU's. DNP3 SA is a critical enabler of Smart Grid technology providing the secure means for command and control of ISO New England's nearly 3000MW of Real-Time Demand Resource starting in June 2010. ISO New England recommends the use of DNP3 SA.

Rationale

DNP Secure Authentication is a recently released addition to the popular Distributed Network Protocol (DNP3) standard¹. For the implementation of the ISO New England Demand Resource Integration Project on June 1, 2010, ISO New England's Communication Front End (CFE) will support DNP3 SA as a configurable option on a per RTU association (session) basis. The ISO-NE CFE will also support regular DNP3 (regular here means DNP3 without Secure Authentication). ISO New England will be basing its DR implementation on the July 31, 2008 version of the DNP3 SA Specification. The specification has been through three years of IEC and DNP open development process. DNP3 SA is in software release form within the industry's most popular DNP protocol stack implementation from Triangle MicroWorks² since September 2008.

DNP3 SA permits the receiver of a DNP3 message (the RTU) to verify that:

- The message came from an authorized user
- The message was not tampered with in transit

NERC firmly believes SCADA should be secured. In 2007, the NERC Control Systems Security Working Group released their Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations. Vulnerability Number Nine is stated as:

9. Control systems command and control data not authenticated

- *Authentication for LAN-based control commands not implemented*
- *Immature technology for authenticated serial communications to field devices.*

NERC's recommended mitigation for this vulnerability is "Use control system protocols that contain appropriate authentication and integrity attributes without affecting performance as the technology becomes available." The DNP Secure Authentication specification is exactly this type of protocol and is based upon NIST and ISO algorithms and techniques.

¹ http://www.smartgridnews.com/artman/publish/industry/DNP_Secure_Authentication_Essential_to_Smart_Grid_Progress.html

² <http://www.tmw-usa.com>

36

37 While it is understood that EPRI-funded vulnerability testing in 2009 has revealed one weakness in the
38 current specification, overall the implementation of DNP3 SA is a major step forward in reducing
39 vulnerabilities and is worthy of prompt industry acceptance and implementations. It is expected that an
40 updated DNP3 SA specification will be released in the next two-three months to address improved state
41 machine logic and will result in relatively minor software and firmware updates.

42 Referenced Documents

43 *ISO New England Demand Resource RTU Specification*

44 Vendor Requirements for implementing DNP3 SA

45 The following describes the minimal Vendor Requirements for implementing DNP3 SA. Two RTU
46 vendors have expressed intentions to release their DNP3 SA products in order to support ISO New
47 England Demand Designated Entities (DDE’s) who are required to purchase RTU’s as specified in the ISO
48 New England Demand Resource RTU Specification document. We are imploring more vendors to
49 release DNP3 SA products for ISO New England’s Demand Resource Smart Grid Integration Project.

50 *DNP Master*

51 The ISO New England DNP Master will support DNP3 SA via Triangle MicroWorks DNP libraries for
52 testing purposes by 08/15/09 in order to perform Inter-Operability Testing with participating RTU
53 vendors. It is expected that Inter-Operability Testing will take place from 08/15/09 to 11/30/09 as well
54 as unstructured testing as time permits. Please note that Inter-Operability Testing will not be exclusive
55 to RTUs that support DNP3 SA.

56 *DNP Outstations*

57 Vendor DNP3 Outstations must meet requirements set forth in the *ISO New England Demand Resource*
58 *RTU Specification* document.

59 Additional requirements for DNP3 Secure Authentication are as follows. Please note that ISO New
60 England has successfully performed preliminary testing between it’s DNP Master and TMW Test Harness

	Outstation SA Function	Requirement	Notes
	Enable/Disable Secure Authentication	Configurable on a per association basis	
	Enable/Disable Aggressive Secure Authentication	Configurable on a per association basis	
	Key Length	AES 128 bit or 256 bit – configurable on a per association basis	This applies for both the Private Key as well as the automatically generated internal Session keys.
	Private (KEK) Configuration	See Notes	Vendors should take necessary steps to ensure that the Key Encryption Key (KEK) is stored in a secure fashion within the

			RTU. Access to the RTU Configuration Utility (vendor specific) must also be secured and not allow for clear text viewing of the KEK.
1	KeyWrap Algorithm	AES 128 Key Wrap Algorithm per RFC 3394 ³	ISO-NE has successfully tested it's DNP Master KeyWrap algorithm implementation against the TMW TH v3.5 as well as the RFC 3394 test vectors. Per the DNP3 SA Spec, this is the only required KeyWrap algorithm at this time.
2	HMAC Algorithm	SHA1 – 4 Octet SHA1 – 10 Octet SHA256 – 8 Octet SHA256 – 16 Octet Configurable	These are the only required HMAC Algorithms at this time. ISO-NE has implemented all four algorithms in it's DNP Master and successfully tested with the TMW TH v3.5.
3	Authenticated Users	Up to ten authorized users are to be allowed. Each user is identified by successively incremented integer starting with '1'	ISO-NE will likely only require one user per association.
	Authorization	None Required	ISO-NE is not requiring that individual authenticated users be allowed configurable authorization level(s) to the outstation.
4	Critical Function Codes	Configurable – See Notes	ISO-NE suggests that <u>all</u> DNP Function Codes be considered critical and subjected to SA
5	Logging	Configurable	ISO-NE suggests that the DNP3 SA state machine be outfitted with logging for various status messages including the ability for external monitoring of SA status including intrusion detection monitoring

61

62 Other important configurable parameters needed for the DNP3 SA Outstation as outlined in the
63 following table.

64 *Please note that there are likely to be additional SA state machine counters and variables added as a*
65 *result of the recent vulnerability testing to decrease the likelihood of a DOS attack in the coming months.*
66 *These counters will be something that would result in an upgrade to the Outstation firmware at a later*
67 *date.*

³ <http://www.ietf.org/rfc/rfc3394.txt>

68

69

Outstation SA Setting	Default	Notes
Authentication Reply Default	2 seconds	
Key Change Interval	15 minutes	This is for Session Key Change not Private Key Change interval. The latter is determined via an administrative procedure
ASDU Count since last (Session) Key Change	1000	
Max Error Count	2	

70