EPRI | ELECTRIC POWER RESEARCH INSTITUTE

DNP3 (IEEE Std 1815™) Secure Authentication

Implementation and Migration Guide and Demonstration Report

3002003736

DNP3 (IEEE Std 1815™) Secure Authentication

Implementation and Migration Guide and Demonstration Report

3002003736

Technical Update, December 2014

EPRI Project Manager

R. King

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

EnerNex, LLC

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

EnerNex, LLC
620 Mabry Hood Road Suite 300
Knoxville, TN 37932

Principal Investigator
G. Gilchrist

This report describes research sponsored by EPRI.

EPRI wishes to thank the organizations listed in Table A-4 on page A-9 for their generous volunteer participation in the 2014 DNP3-SA Interoperability Demonstration.

This publication is a corporate document that should be cited in the literature in the following manner:

DNP3 (IEEE Std 1815™) Secure Authentication: Implementation and Migration Guide and Demonstration Report. EPRI, Palo Alto, CA: 2014. 3002003736.

PRODUCT DESCRIPTION

This report is intended to be a tutorial accompaniment to the Institute of Electrical and Electronics Engineers (IEEE) Std 1815™, also known as the Distributed Network Protocol (DNP3). This report focuses on the Secure Authentication features of the standard (DNP3-SA), and provides guidelines on how utilities can best design, implement and migrate toward using these cyber-security features. The report also describes the objectives, implementation and results of a multi-vendor interoperability demonstration organized by the Electric Power Research Institute (EPRI) in 2014 that illustrated compatibility between existing DNP3-SA products and devices.

Background

DNP3 is the most widely used utility communications protocol in North America. It has been released as the IEEE 1815 standard and is recognized in the National Institute of Standards and Technology (NIST) Smart Grid Interoperability Framework as one of the key standards to be used in smart grid deployments. Therefore, ensuring that DNP3 communications are secure is an important goal for the power industry.

A tutorial of the type found in this report, and the interoperability demonstration described here both serve to increase utility knowledge about the DNP3-SA technology, and encourage utilities to feel comfortable specifying it in evaluation projects.

Objectives

To increase utilities' knowledge of the DNP3 standard and make them aware of important options and issues they should consider when migrating their networks toward using DNP3-SA.

Approach

The guidelines in this report are a collation and enhancement of several documents produced by the DNP3 Users Group, plus the addition of tutorial material to provide examples and recommendations. The demonstration described in this report was organized through a series of web conferences starting in June 2014, with a vendor interoperability "plug-fest" in September, and a workshop summarizing the results for utilities in November 2014. The objectives of the EPRI DNP3-SA demonstration in 2014 were:

- To demonstrate the basic functions of DNP3-SA.
- To demonstrate co-existing DNP3-SAv2, DNP3-SAv5, and non-secure environments.
- To demonstrate a complete system, including cryptographic key management. Cryptographic key management was a particular challenge because the interface between some of the components had not yet been designed. This project performed much of that design and laid the groundwork for standardizing the interface.
- To identify areas that may need clarification in the specification.

Results

This report provides example scenarios of various possible cryptographic key management designs and discusses their benefits and disadvantages. It discusses how DNP3-SA can be deployed in the context of other security measures. It recommends software issues to discuss

with vendors, and includes scenarios and concerns when migrating from non-secure DNP3 or DNP3-SA version 2 to DNP3-SAversion 5.

The EPRI DNP3-SA demonstration project defined 192 scenarios in the categories of topology, protocol, and key management. Eleven vendors successfully tested 162 of these scenarios, or 84%, in a three-day interoperability "plug-fest." Only two incompatibilities and three implementation errors were found. Fifteen of the successful scenarios were demonstrated at EPRI's DNP3 Technology Transfer Workshop.

Applications, Value, and Use

This report describes the basics of how DNP3-SA works, and the design choices that must be made by utilities to deploy it. It is best used by managers who are responsible for deploying power utility communications networks to evaluate the choices and steps necessary to deploy DNP3-SA.

Keywords

Authentication
Certificate
Credential
Cyber security
Interoperability
Cryptography
Security
SCADA

ABSTRACT

This report is intended to be a tutorial accompaniment to the Institute of Electrical and Electronics Engineers (IEEE) Std 1815 ™, also known as the Distributed Network Protocol (DNP3). This report focuses on the Secure Authentication features of the standard (DNP3-SA), and provides guidelines on how utilities can best design, implement and migrate toward using these cyber-security features. The report also describes the objectives, implementation and results of a multi-vendor interoperability demonstration organized by the Electric Power Research Institute (EPRI) in 2014 that illustrated compatibility between existing DNP3-SA products and devices.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
BASICS OF DNP3-SA

This document focuses on the security extensions to the DNP3 protocol, referred to as DNP3 Secure Authentication (DNP3-SA). DNP3 SA provides application layer functions and data objects that permit devices to authenticate DNP3 communication messages by verifying the source of the message and that the message was transmitted without modification.

DNP3 Secure Authentication Version 2 (SAv2) was first released as part of IEEE Std 1815-2010. DNP3-SAv2 has been deprecated and superseded by DNP3 SA Version 5 (SAv5) included in the most recent release of the DNP3 standards (IEEE Std 1815-2012) [1].

DNP3-SA is based on the international standard IEC 62351-5 [2], which in turn is based on several different standards issued by the International Standards Organization (ISO), International Electrotechnical Commission (IEC) the Internet Engineering Task Force (IETF) and the U.S. National Institute of Standards and Technology (NIST).

1.1 Threats Addressed by DNP3-SA

DNP3-SA is primarily focused on the threats to authenticity and integrity of the data being exchanged such as:

- **Spoofing** – impersonating an authorized user or device
- **Modification** – changing messages in transit
- **Replay** – capturing a valid message and retransmitting it at an inappropriate time
- **Eavesdropping** – capturing private or secret information in transit. DNP3-SA provides protection from eavesdropping on exchange of cryptographic keys only, not on normal DNP3 messaging.

1.2 Why Use DNP3-SA?

There are three types of security that are commonly deployed in communications networks today, as illustrated in:

- **Site-to-Site Security**: Site-to-Site Security includes the use of Virtual Private Network (VPN) routers and protocols such as IPSec to secure the link between two locations, e.g., a corporate office and a home office, or a master station and a substation. Since the IPSec tunnel is typically terminated at the border of each network, it does not secure the networks at those two locations, and physical security measures such as locks and guards are necessary to protect them.
- **Device-to-Device**: Device-to-Device security can include the use of protocols such as Transport Layer Security (TLS) to secure the complete TCP connection between two devices, similar to when you access your bank through the Internet. However, TLS only works on IP networks and is therefore not implemented if DNP messages are forwarded over radios or serial links. TLS also does not address the possibility that rogue software

applications may be installed on a device, making use of the fact that the device itself is considered secure.

- **Application-to-application**: Application-to-application security ensures that individual users, not just devices, are authenticated by the remote devices, and that the authentication information will be carried wherever the DNP3 message travels. This permits remote outstations to perform role-based authentication and authorization so that the level of security changes depending on who is attempting to perform an operation.

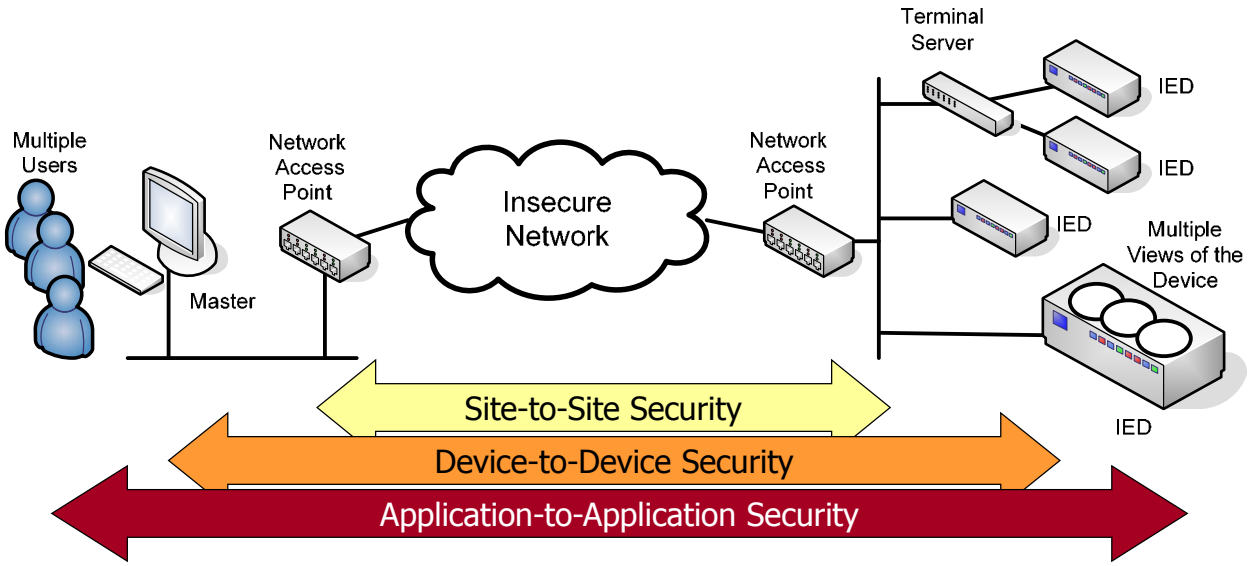

Figure 1-1
Comparison of DNP3-SA (Application Security) to Other Types of Security

The primary benefit of implementing DNP3-SA is that it is an application-to-application security solution. DNP3 is challenging to secure because it can be used in a variety of networks, including radio systems, serial links, and IP-based wide-area networks. It is not uncommon that from master to outstation, DNP3 traffic may traverse more than one of these types of communications links. For this reason, DNP-SA is included in the topmost of the OSI layers, the application layer.

1.3 How Does DNP3-SA Work?

The DNP-SA mechanism is based on the concept of a "cryptographic hash." A hash is a function similar to a Cyclic Redundancy Check (CRC) or a checksum, that when performed on a message, produces a much smaller string of numbers. This smaller hash value is very sensitive to changes in the message, and it is virtually impossible to determine the original message if all you have is the hash value.

As an example, referring to Figure 1-2, "Alice" is trying to send a message to "Bob" in a way that Bob can be sure the message is authentic. To make it work, Alice and Bob must have previously shared a cryptographic key [hereafter referred to as the key], a string of numbers that only the two of them know.

1. Alice appends the key to the end of the message and **performs the hash function** on the resulting longer block of data. This produces a small hash value.
2. **Alice sends the original message and the hash value to Bob.** She does NOT send the key, because it could be seen by an attacker. However, the message is not encrypted in this case. The attacker can see the message, but cannot modify it without being detected or send a false message of the attacker's own.
3. **Bob receives the message.** Since he already has a copy of the key, he can now duplicate Alice's calculation. He produces a hash value using the key.
4. If Bob's hashed value matches the value that Alice transmitted with the message, he knows two things:

- **The message has not been modified.** If an attacker had tampered with the message, Bob's calculation would have been on a different message than Alice used, and therefore the hash value would have been different. The hash function is carefully designed so that without knowing the key, an attacker could not modify the message in such a way that would produce a correct hash.
- **The message came from Alice** – or at least, someone who knew the pre-shared key. Although the key was not transmitted on the link, it was intrinsic to the calculation and without it, an attacker could not produce a matching hash value. Because of the way the hash works, it is nearly impossible to determine the key from the hash value.

When a hash is used with a key in this manner, it is known as a **Message Authentication Code, or MAC.**

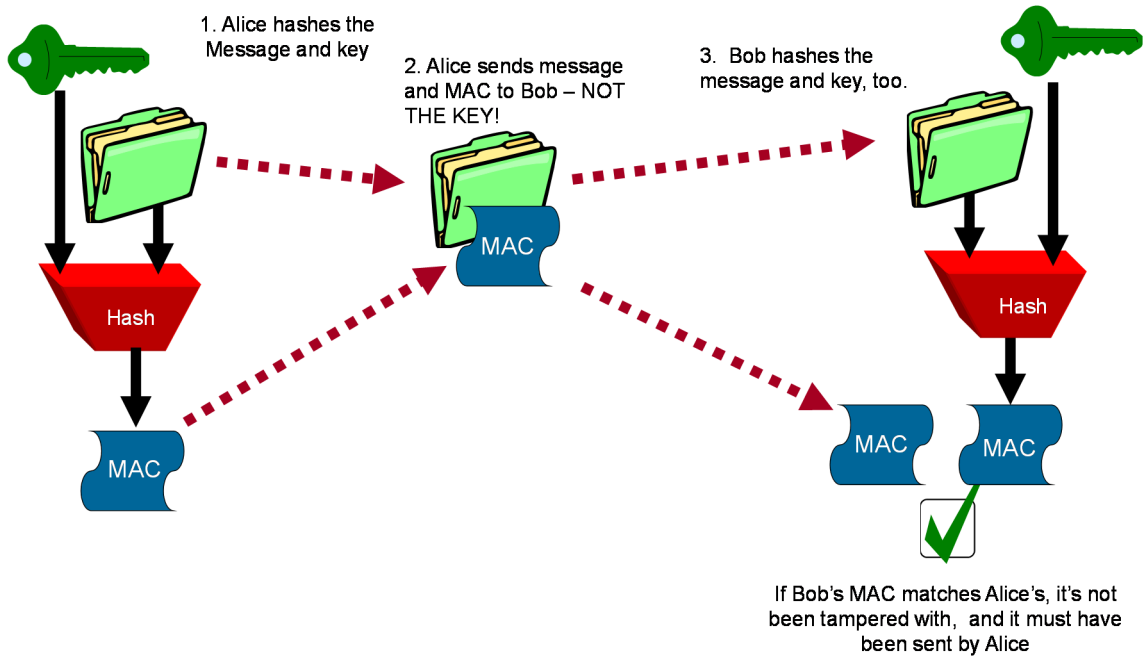

Figure 1-2
Basic Authentication in DNP3-SA using MACs

The other basic principle used in DNP3-SA is that of Challenge-Reply, as illustrated in Figure 1-3. Any device may send an authentication challenge containing random data in response to a normal DNP3 message such as a control operation. The device that sent the DNP3 message (the master in the case of a control) must then reply with a MAC calculated over the original message, the current cryptographic Session Key, and the random data from the challenge. If the challenger (the outstation in the case of a control) calculates that the MAC is valid, it performs the operation. There is also an "aggressive mode" in which the MAC is "piggy backed" on the end of the original operation, to reduce the number of messages sent.

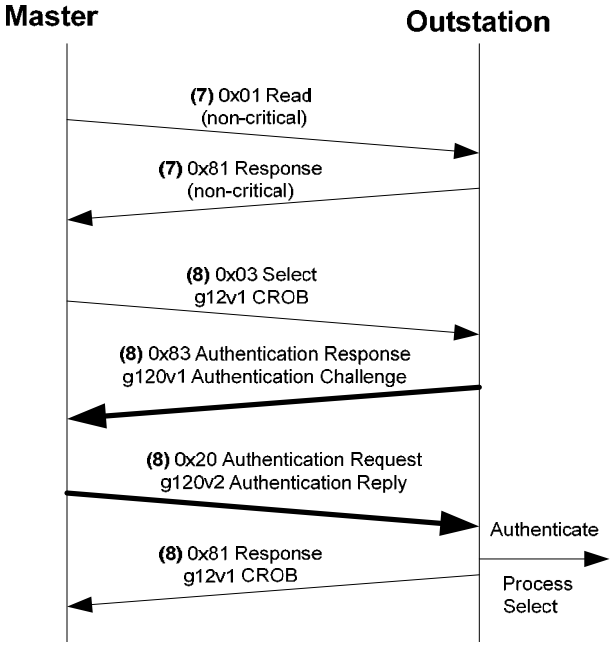

Figure 1-3
Example of Challenge-Reply, Extracted from IEEE Std 1815-2012

1.4 Where Should DNP3-SA Be Applied?

DNP3-SA can be applied anywhere that DNP3 is currently used. However, it has several particular advantages in the following areas:

- **Mixed serial-and-IP networks.** The IEEE Std 1815-2012 defines the networked version of DNP3 as the serial version of DNP3 encapsulated in a TCP stream or a UDP packet. Therefore, since it operates at the DNP3 application layer, DNP3-SA can provide end-to-end security over a mixed network using third-party generic terminal servers, as shown in Figure 1-4. This scenario was successfully tested at the 2014 EPRI DNP3 Interoperability Demonstration (See Appendix A).
- **Low bandwidth, low-processing power systems.** DNP3-SA is designed particularly for supervisory control and data acquisition (SCADA) systems in which communications links may have limited bandwidth and devices may have limited processing power. For instance, DNP3-SA supports symmetric-only cryptography, which often requires hundreds of times less processing power than asymmetric cryptography. It also does not mandate the use of encryption, just authentication, which further reduces processing requirements. And it supports an Aggressive Mode which reduces the number of messages and the size of messages required to perform authentication.

- **Upgraded non-secure DNP3 systems.** DNP3-SA can be implemented entirely in software and does not require special hardware. If the devices in question can handle the additional processing power needed, and the firmware can be upgraded, the change to DNP3-SA can be a software-only change.

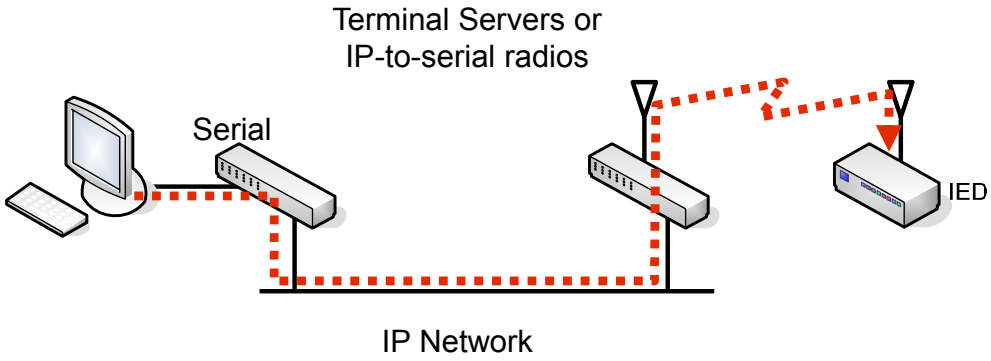

Figure 1-4
Example of using DNP3-SA in Mixed Serial and IP Networks

2
DESIGN CHOICES

This section describes the important design choices that must be made by utilities planning to implement DNP3-SA. Many of these choices are also described in the DNP3-SA Tutorial, available on the DNP Users Group web site (www.dnp.org) to Users Group members. Figure 2-1 illustrates a flowchart for addressing the key management design choices described in later parts of this section.

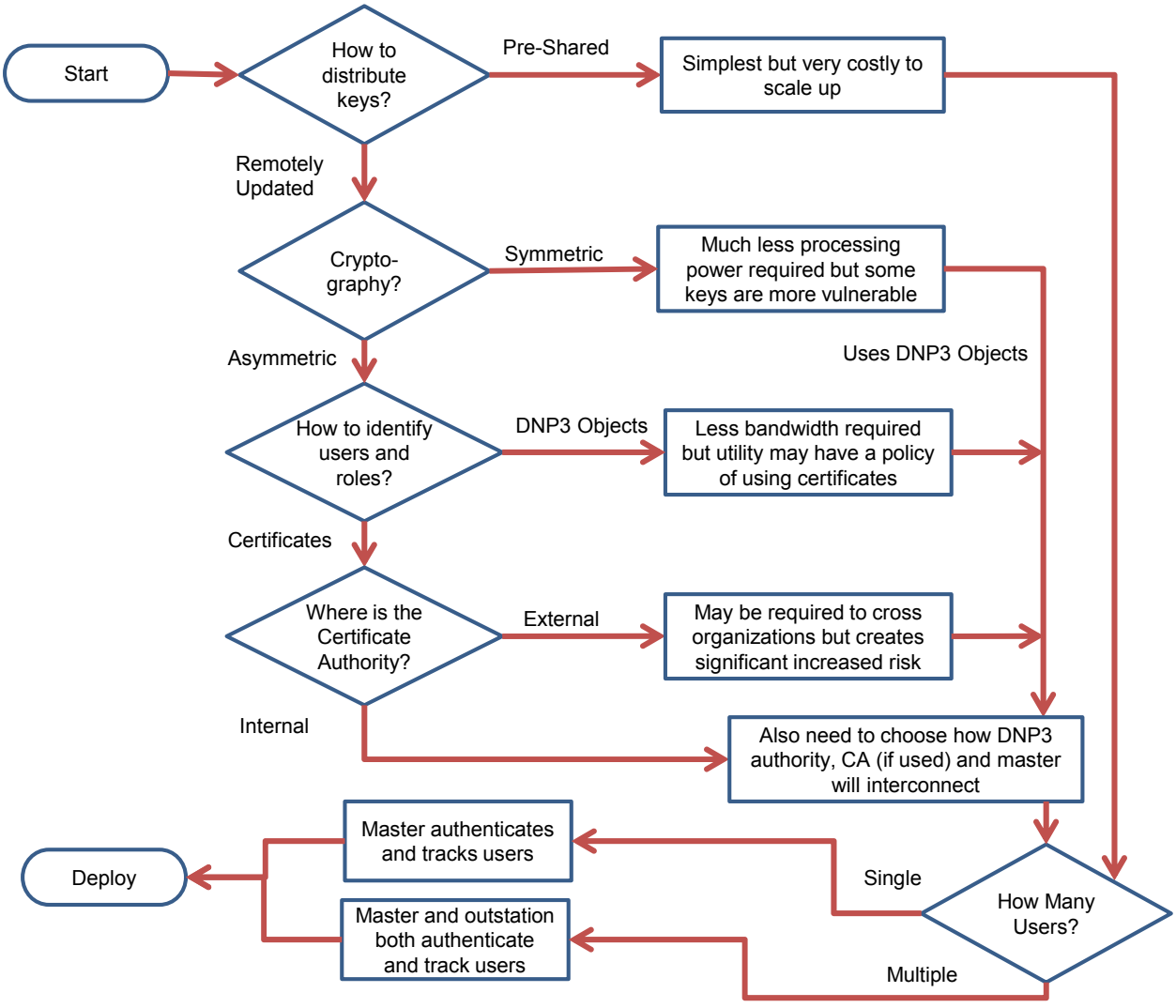

Figure 2-1
Summary of Key Management DNP3-SA Design Choices to Be Made By Utilities

2.1 Protocol Stack

DNP3-SA may be used over both serial and IP networks. Utilities must choose the appropriate protocol stack based on where they want to use DNP3-SA.

When used over serial links or radio systems, the authentication function codes and objects are carried the same as any other DNP3 traffic.

When used over IP networks, there are three different options, as illustrated in Figure 2-2.

- **TCP with authentication only**, recommended for use over wide-area networks and mixed networks
- **UDP with authentication only**, recommended for reliable local area networks only
- **TCP with authentication and encryption using Transport Layer Security**, recommended if messages must travel over an insecure network such as the Internet.

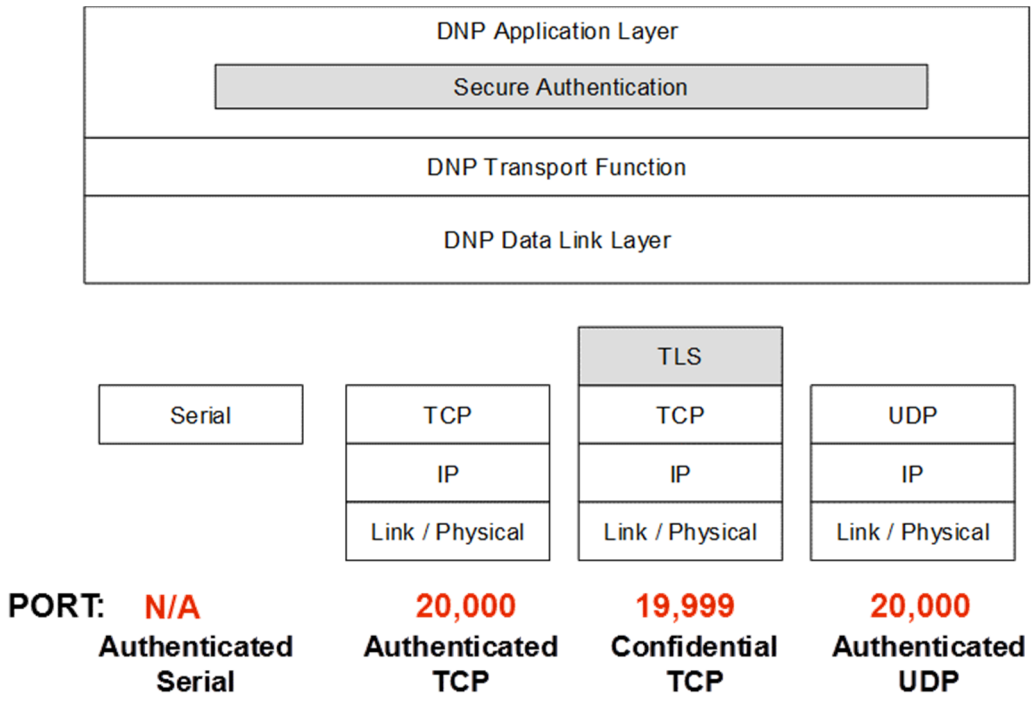

Figure 2-2
DNP3-SA Protocol Stacks

2.2 Critical Functions

Not all DNP3 functions are required to be authenticated when implementing DNP3-SA. Table 7-7 within IEEE Std 1815-2012 identifies a minimum subset of functions that shall be considered critical. Utilities may choose to designate additional DNP3 functions, beyond those considered as mandatory, as critical within their specific implementations.

Table 2-1
DNP3 Critical Request Function Codes (Extracted from Table 7-7 of IEEE Standard 1815-2012)

Function Code		Description	Critical
Decimal	Hex		
0	0x00	Confirm	optional
1	0x01	Read	optional
2	0x02	Write	MANDATORY
3	0x03	Select	MANDATORY
4	0x04	Operate	MANDATORY
5	0x05	Direct Operate	MANDATORY
6	0x06	Direct Operate – No Acknowledgement	MANDATORY
7	0x07	Immediate Freeze	optional
8	0x08	Immediate Freeze – No Acknowledgement	optional
9	0x09	Freeze-and-Clear	optional
10	0x0A	Freeze-and-Clear – No Acknowledgement	optional
11	0x0B	Freeze-at-Time	optional
12	0x0C	Freeze-at-Time – No Acknowledgement	optional
13	0x0D	Cold Restart	MANDATORY
14	0x0E	Warm Restart	MANDATORY
15	0x0F	Initialize Data (obsolete)	optional
16	0x10	Initialize Application	MANDATORY
17	0x11	Start Application	MANDATORY
18	0x12	Stop Application	MANDATORY
19	0x13	Save Configuration (deprecated)	MANDATORY
20	0x14	Enable Unsolicited Responses	MANDATORY
21	0x15	Disable Unsolicited Responses	MANDATORY
22	0x16	Assign Class	optional
23	0x17	Delay Measurement	optional
24	0x18	Record Current Time	MANDATORY
25	0x19	Open File	MANDATORY
26	0x1A	Close File	MANDATORY
27	0x1B	Delete File	MANDATORY
28	0x1C	Get File Information	MANDATORY
29	0x1D	Authenticate File	MANDATORY
30	0x1E	Abort File	MANDATORY
31	0x1F	Activate Configuration	MANDATORY
32	0x20	Authentication Request	Not applicable
33	0x21	Authentication Request – No Acknowledgement	Not applicable
129	0x81	Response	optional
130	0x82	Unsolicited Response	optional
131	0x83	Authentication Response	Not Applicable

2.3 Pre-Shared vs. Remotely Updated Keys

This is the first key management design decision illustrated in the flowchart in Figure 2-1 on page 2-1. Utilities planning to implement DNP3-SA must choose between using pre-shared (i.e. pre-configured) or remotely updated keys. While the initial version of DNP3-SA (SAv2) specified only the use of pre-shared keys, the option of remotely changing Update Keys was added in DNP3-SAv5. The reason this topic tends to be controversial is a matter of risk and cost. While the use of pre-shared keys may present a simpler solution on the front end of a utility deployment, it may result in increased risk and cost in the long run.

- Risk, in that it is more likely that Update Keys would be compromised by someone leaving a utility organization than by an attacker cracking the keys on the link.
- Cost, in that there are a large number of devices in the typical SCADA system, and the manual distribution of new keys to all these sites would be prohibitive.

For these reasons, it is recommended that DNP3-SA implementations support the ability to remotely change Update Keys.

Public key cryptography is currently the approved mechanism in the computer industry for reducing the risk and cost associated with key changes. However, the utility industry has topology and processing power concerns that may make public key cryptography excessively costly.

2.4 Symmetric vs. Asymmetric Keys

This is the second key management design decision illustrated in the flowchart in Figure 2-1 on page 2-1. Utilities electing to remotely change Update Keys must also choose whether symmetric or asymmetric cryptography is utilized. Keys are managed from a central authority using either:

- Pre-shared (symmetric) keys
- Asymmetric keys, also known as public key encryption

In symmetrical cryptography, the same key is utilized on both ends of the message exchange. Because of the inherent risk of the key being compromised, symmetrical keys must be exchanged using out-of-band communications. That typically means physically sending someone to each location and pre-configuring the keys.

In asymmetrical encryption, a pair of keys (public key and private key) is created for each node. The public key is distributed for each node while the private key is kept secret. To send an encrypted key to a designated node, the sender uses the recipient's public key to encrypt the key. Once encrypted, only the secured private key can be utilized to decrypt the key. Although it is considered the preferred solution for most commercial computing today, asymmetrical key encryption is processing-intensive and may not be compatible for retrofit into older legacy systems.

Within IEEE Std 1815-2012, the symmetric method is the mandatory default while asymmetric methods are optional. The current best practice is considered a hybrid of the two approaches that uses asymmetric keys for initial authentication and also for the subsequent exchange of symmetric session keys.

2.5 Single-User vs. Multi-User

Another important decision that utilities must make when developing the DNP3-SA implementation plans is that of single-user or multi-user authentication. This is shown as the last key management design decision illustrated in Figure 2-1 on page 2-1, but it may not be the last decision made. The utility must keep this in mind throughout the design process.

In a multi-user configuration, when a user initiates a critical operation that sends DNP3 messages from a master station to the outstation, the master station is responsible for identifying and authenticating the specific user and utilizing the associated valid Session Keys for that user. The outstation is responsible for validating the Session Keys based on the Update Key for that user, and can enforce privileges based on the role of the user. In a multi-user scenario, user names and Update Keys are typically managed within the central authority and must be unique within the organization; however, they can also be pre-configured.

In a single-user configuration, the master station appears to the outstation as a single user. If a utility requires traceability of an action back to a specific user in this scenario, it must rely solely on the functionality within the master station to authenticate all users and log all user activity independent of the DNP3-SA implementation.

2.6 Assignment of Roles

If a utility has elected to implement a multi-user configuration, the next decision that must be made is to define the privileges of each user to develop the overall role based access control scheme. Table 2-2 outlines the user roles definitions within DNP3-SA specifications. These roles are aligned with roles defined within IEC 62351-8 [3] and assigned within the central authority. No user is permitted to change the Role of another user; only the authority may change roles.

2.6.1 Standard Roles

DNP3-SA makes use of seven standardized roles and privileges (User Role = 0 – 6 in Table 2-2).

2.6.2 Non-Standard Roles

The DNP3-SA specifications leave open the option for the utility to define non-standard roles beyond those defined within the standard (User Role = 32769 – 65535 in Table 2-2). If a utility elects to define non-standard roles within its DNP3-SA architecture, it may be necessary to validate interoperability of the devices that must support them.

2.6.3 The SINGLEUSER Role

The DNP3-SA specifications also provide for a role defined as “SINGLEUSER” (User Role = 32768 in Table 2-2) that provides all possible privileges to a user. This should not be used as the default role for users defined within the central authority.

Table 2-2
DNP3-SA User Roles (Extracted from Table 7-12 of IEEE Std 1815-2012)

Value	Name	Permissions						
		Monitor data	Operate controls	Transfer data files	Change config	Change security config	Change code	Local login
<0>	VIEWER	Yes	No	No	No	No	No	No
<1>	OPERATOR	Yes	Yes	No	No	No	No	No
<2>	ENGINEER	Yes	No	R/W/D	Yes	No	No	Yes
<3>	INSTALLER	Yes	No	R/W	Yes	No	Yes	Yes
<4>	SECADM	No	No	No	No	Yes	Yes	Yes
<5>	SECAUD	Yes	No	R	No	No	No	Yes
<6>	RBACMNT	Yes	No	D	Yes	Roles only	No	No
<7..32 767>	RESERVED	For future use.						
<32 768>	SINGLEUSER	Yes	Yes	R/W/D	Yes	Yes	Yes	Yes
<32 769 .. 65 535>	PRIVATE	Defined by external agreement. Not guaranteed to be interoperable.						

2.7 Certificates vs. Non-Certificate

This is the third key management design decision illustrated in the flowchart in Figure 2-1 on page 2-1. If utilities choose to remotely change Update Keys using asymmetric cryptography, they must then choose one of the following options for identifying the user to an outstation and changing the user's role or status:

- **Standard certificates.** A cryptographic certificate is a digitally signed electronic document that certifies a particular user is associated with a particular public key, and for how long. The international standard for the format of certificates is the International Telecommunications Union (ITU) X.509 standard. DNP3 uses enhancements to the X.509 standard defined by the International Electrotechnical Commission (IEC) 62351-8 standard. These enhancements include being able to specify the role of the user, as discussed in the previous section of this report. When the master sends a certificate to the outstation, it is transmitted in a User Certificate (g120v8) object.
- **DNP3 objects (non-certificate).** One drawback of certificates is that they can sometimes be quite large by comparison with other data sent on a utility communications network. To conserve bandwidth, DNP3-SA also provides a method for sending the same information that would be contained in a certificate (user name, public key, role, and expiry) within as few octets as possible. Instead of a User Certificate Object, the master transmits a User Status Change (g120v10) object.

A utility should choose one of these methods based on whether it is practical to send certificates on the communications network to the outstation, and whether the utility is already using certificates as credentials within the organization. Many utilities already have internal requirements for using certificates as security credentials.

2.8 Internal vs. External Certificate Authority

If utilities choose to remotely change Update Keys using standard certificates, they must then choose whether to use an internal or external certificate authority. This is the fourth key management design decision illustrated in the flowchart in Figure 2-1 on page 2-1.

In DNP3-SA, a certificate is a document that tells an outstation to recognize a user as a valid user of that outstation and that the user's public key and role are valid for a specific length of time. The certificate must be digitally signed by a "certificate authority" that the outstation is pre-configured to recognize. Usually this configuration is performed by supplying the outstation with the self-signed certificate of the certificate authority. There are generally two choices for a utility:

- **Internal Certificate Authority.** Software is available that would permit a utility to be its own certificate authority. This option is likely to be preferred by most utilities because it gives them complete control over user access to outstations.
- **External Certificate Authority.** It is possible to have external organizations act as certificate authorities. The utility would have to submit information (the names, roles and expiry dates of users) for signing by the external authority. This option is generally only useful if users must be recognized not only by the utility but also by some other organization.

2.9 Relationship between DNP3 Authority, Certificate Authority, and Master

If utilities choose to remotely update keys using standard certificates, they must then choose how the certificate authority and the DNP3-SA authority will be related. This choice may be dependent on what products are available.

There are generally five different software entities participating in managing keys using certificates in DNP3-SA:

- The **DNP3 Authority** stores information on which users have privileges on which outstations, with which roles, for how long.
- The **Certificate Authority** digitally signs documents (certificates) stating that the information stored and distributed by the DNP3 Authority is accurate. If a utility chooses to use symmetric cryptography or chooses to use asymmetric cryptography without certificates, there is no certificate authority.
- The **Master** forwards certificates and other information from the DNP3 Authority to the outstation and interleaves it with the other DNP3 data transmitted to and from the outstation.
- The **Outstation** is pre-configured to recognize the signature of the certificate authority and enforces the roles and privileges of users.
- The **User** logs into the master and may carry his/her own keys and certificates on a security token.

The IEEE Std 1815-2012 specifies only the messages between the master and the outstation. It proposes the data to be exchanged between the DNP3 Authority and the master, but does not define the exact message format. It does not discuss the relationship between the DNP3 Authority and the Certificate Authority. These omissions were intentional, to limit the scope of the specification to the DNP3 protocol only.

To begin to address these omissions, the participants in the EPRI DNP3-SA Interoperability Demonstration held in 2014 (see Appendix A) began defining the DNP3 Key Management Protocol (DKMP) and a proposal for the procedures to be used between the four entities. The proposed data flow between the entities is illustrated in Figure 2-3.

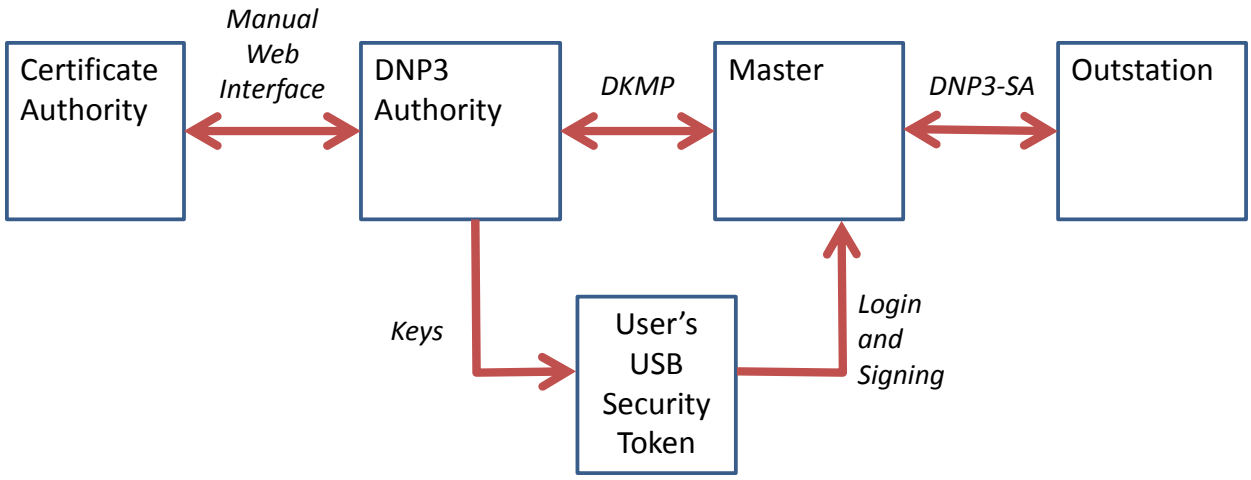

Figure 2-3
Proposed Data Flow in DNP3-SA Cryptographic Key Management

The steps in the proposed procedures are illustrated in Figure 2-4.

This process and the DKMP are not yet a standard, although they may be submitted for consideration as a standard in the near future. Some of the interfaces to a certificate authority are defined in the Public Key Certificate Standards (PKCS) specifications. For instance, a Certificate Signing Request (CSR) is RFC 2986 and was used in the demonstration. However, not all of the PKCS specifications are recognized as standards.

It is expected that some DNP3 Authority software products may include their own certificate authority, and may be bundled with the DNP3 master software. Until these interfaces are standardized, utilities will have to decide on the relationship between these entities based on what products are available.

2.10 Revoking Certificates

If utilities choose to remotely change Update Keys using standard certificates, they must provide a mechanism for revoking certificates. Certificates may be revoked for a number of reasons: for instance if the utility believes a private key has been compromised, or if the person named in the certificate is no longer trusted, or if a security policy has been violated. The following are two common ways revocation might be performed, although they are not the only possible methods:

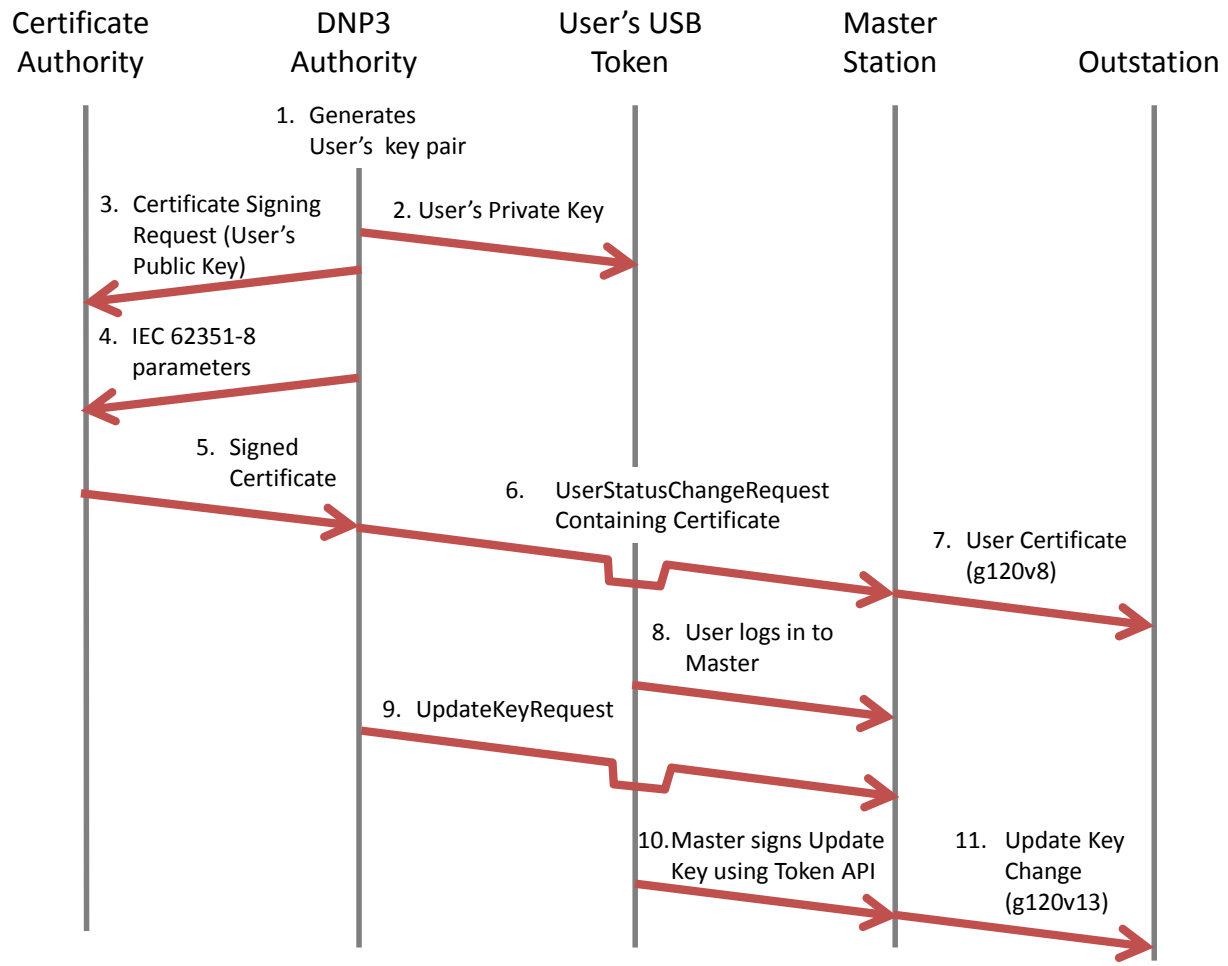

Figure 2-4
Key Management Process from EPRI 2014 DNP3-SA Interoperability Demo

- **Certificate Revocation Lists (CRLs).** This is the traditional method for revoking certificates. A list of revoked certificates is published periodically by the certificate authority or some other entity trusted by the certificate authority. Before using a certificate, software should check the most recent version of the certificate revocation list.
- **Online Certificate Status Protocol (OCSP).** This is a more recent method for detecting revoked certificates. OCSP defines messages that permit a software client to query whether a particular certificate has been revoked, whenever the client needs the information. OCSP has at least two advantages over CRLs:
  - It does not require transmitting the entire revocation list, (which can grow quite large)
  - It is easy to check the latest database of revoked certificates at the moment the certificate must be used.

The IEEE Standard 1815-2012 does not define how or when certificates should be revoked or checked. There are a few possible options:

- The **outstation** could check whether a certificate is revoked just before using it, namely when it is about to download the Update Key for the user specified in the certificate. However, this would require that the outstation have an ability to periodically download a CRL or send an OCSP query from a server. Many outstations may not have the physical access to such a server; their only access is via the DNP3 link.
- The **master** could check whether a certificate is revoked just before sending it to the outstation. The master is more likely to have access to the appropriate server. This is more likely to be the preferred choice of utilities, especially those whose DNP3 devices are accessed via serial links. Utilities should verify that their master station products support this capability, and investigate whether the master uses CRLs or OCSP.

2.11 Configuration Parameters

This section describes some of the configuration parameter choices that utilities must make to deploy DNP3-SA. Table 2-3 lists some typical values for the various parameters.

Table 2-3
Typical DNP3-SA Configuration Parameters

Parameter	Typical Value	Notes
Secure Authentication Version	5	Version 2 is no longer recommended for new installations
Outstation Name	Text string	Chosen by the utility per outstation, configured at master if Update Keys are downloaded
User and Outstation Areas of Responsibility	Text strings	Chosen by utility if using certificates
Keys and Algorithms		**Must match on master and outstation**
MAC Algorithm	<4> HMAC-256 truncated to 16 octets	HMAC-SHA-1 is not recommended any longer and implementations must be able to disable it. Less truncation (more octets) provides better security. GMAC provides better performance but is less commonly available.
Session Key Length	128 bits	128 bits is the minimum; more bits provides better security but will require more processing power
Update Key Length	128 bits (symmetric)	Same as Session Key Length, but note that Update Key operations occur far less often than Session Keys (months vs. minutes)
Key Wrap Algorithm	AES-256 Key Wrap	This is the only algorithm defined in the spec.
Update Key Change Method	<4> Symmetric AES-256 / HMAC-SHA-256	This is the parameter that selects the key management option discussed in section 2: symmetric vs. asymmetric. Asymmetric key lengths longer than 2048 are not yet practical in processing power in most situations.

Table 2-3
Typical DNP3-SA Configuration Parameters (Continued)

Parameter	Typical Value	Notes
Protocol Features		
Use of Error Messages	Enabled	If disabled, the master and outstation will simply not respond if an error such as an authentication failure occurs. This may help reduce the impact of denial-of-service attacks.
Aggressive Mode	Enabled	If disabled, DNP3-SA will use much more bandwidth and perhaps provide somewhat better replay protection because random challenge data is generated more often. However, even with Aggressive Mode Enabled, replay protection is good, so Enabled is the recommended setting.
Number of Users	1	This parameter is discussed in Section 2.
User Status Change Method	Non-Certificate Method	This parameter is discussed in Section 2.
Timers		
Reply Timeout (sec)	5	This is a general DNP3 parameter also sometimes called a Response Timeout. Should be set longer if the latency on communications links is long. Should be about the same for both masters and outstations.
Session Key Change Interval (sec) – Master	900	The expected interval and count on the outstations should be at least twice that configured on the master.
Session Key Change Count – Master	1000	Use message counts rather than seconds on networks that are configured for very infrequent communications.
Expected Session Key Change Interval (sec) – Outstation	1800	The expected interval and count on the outstations should be at least twice that configured on the master.
Expected Session Key Change Count – Outstation	2000	Use message counts rather than seconds on networks that are configured for very infrequent communications.
Maximum Session Key Status Count	5	Setting this value smaller provides more protection against denial-of-service attacks but could cause the master to back off excessively on Session Key changes if set too small.

Table 2-3
Typical DNP3-SA Configuration Parameters (Continued)

Parameter	Typical Value	Notes
Protocol Behavior Throttles		These values throttle or set a limit on how strongly and how often the protocol reacts to error conditions. Setting these parameters to smaller values provides earlier detection and reaction to some kinds of attacks but could make the protocol much less efficient if error conditions such as lost messages or device restarts are occurring very often naturally. This can happen, for instance, when a system is being installed for the first time.
Max Authentication Failures	5	
Max Reply Timeouts	3	
Max Authentication Rekeys	3	
Max Error Messages Sent	10	
Max Rekeys Due to Restarts	3	
Statistics Reporting Thresholds		These threshold parameters are used only to determine how often security statistics should be reported from the outstation to the master. In general, the typical values shown here are set larger for events that are expected to occur more often on a normal system. Failure conditions should be reported more quickly than normal operations.
Unexpected Messages	3	
Authorization Failures	5	
Authentication Failures	5	
Reply Timeouts	3	
Rekeys Due to Authentication Failure	3	
Total Messages Sent	100	
Total Messages Received	100	
Critical Messages Sent	100	
Critical Messages Received	100	
Discarded Messages	10	
Error Messages Sent	10	
Error Messages Rxed	10	
Successful Authentications	100	
Session Key Changes	10	
Failed Session Key Changes	5	
Update Key Changes	1	
Failed Update Key Changes	1	
Rekeys Due to Restarts	3	

3
EXAMPLE SCENARIOS

This section describes examples of several sets of the previously described design choices, ranging from simplest to most complex, and describes their advantages and disadvantages.

3.1 Single User, Single Pre-shared Key, Symmetric Cryptography

The simplest deployment scenario for DNP3-SA is to use a single pre-shared (i.e. pre-configured) Update Key for the whole system, as illustrated in Figure 3-1. A single Update Key is used by the master to communicate with each outstation, and the same Update Key is configured at each of the outstations. Since all the keys are pre-configured, all cryptography used is symmetric. Asymmetric cryptography is only used in DNP3-SA to remotely change Update Keys.

Users are authenticated by the master using some mechanism unrelated to DNP3, such as passwords. There is no DNP3 Authority involved, although the master may query some non-DNP3 directory server using a technology such as RADIUS, LDAP or Kerberos to perform the authentication. The master is also responsible for enforcing the role of each user; for instance, preventing non-operators from performing control operations. To the outstations, all the users (Alice, Bob and Donald) appear to be a single default user.

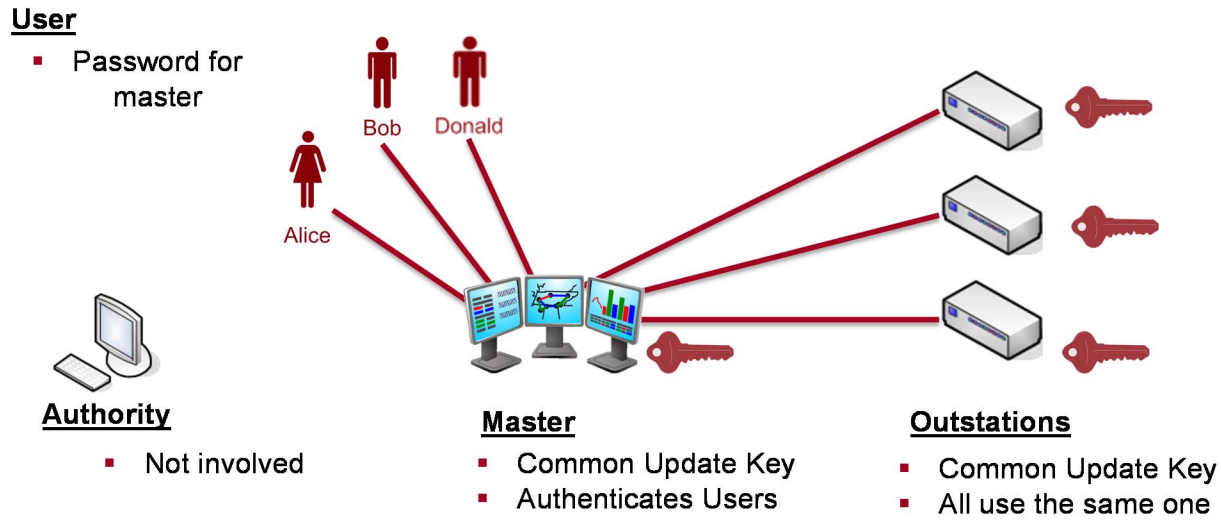

Figure 3-1
Single User, Single Pre-shared Key Scenario

This is the easiest scenario to implement, but is the most vulnerable from a security point of view. If any of the outstations or the master is compromised, the attacker has acquired access to the entire network. Furthermore, if an employee who has access to the Update Keys on the master leaves the organization, the master and all the outstations must, according to security best practices, have their Update Keys changed. This can be a very labor-intensive and costly process.

3.2 Single User, Pre-shared Key per Device, Symmetric Cryptography

The next most secure DNP3-SA deployment scenario is illustrated in Figure 3-2. The master uses a different Update Key to initialize Session Keys on each outstation. In the example, instead of a single Update Key used by the whole system, there are now three, one for each outstation. All keys are still pre-configured. The master is responsible for authenticating users and appears as a single user to the outstations as before.

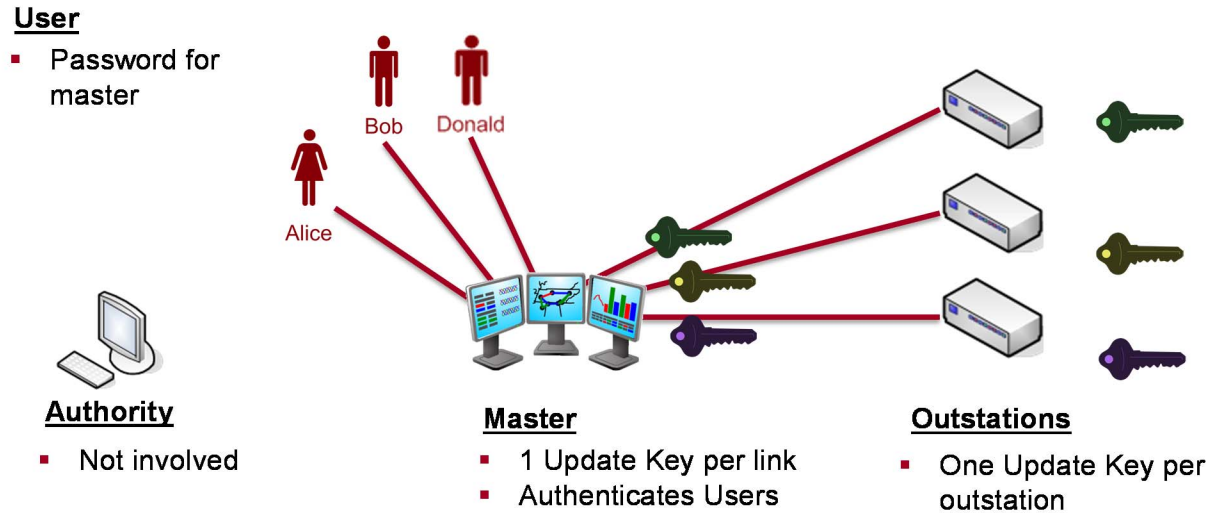

Figure 3-2
Single User, Pre-shared Key per Device Scenario

This scenario reduces the risk from an outstation being compromised compared to the previously discussed scenario. If an attacker breaks into an outstation and retrieves the Update Key configured there, the attacker can impersonate the master to that outstation – but only to that specific outstation. The attacker cannot gain access to any of the other outstations or impersonate those outstations.

Unfortunately, in this scenario there is still the risk of an attacker gaining access to the master, or the risk of an employee with access to the Update Keys leaving the organization. Either of those events would require physical trips to all the outstations to change the Update keys. As with all the pre-shared key scenarios, this type of deployment would not scale well to large numbers of outstations.

3.3 Multiple Users, Pre-shared Keys, Symmetric Cryptography

This scenario adds multiple users to the DNP3-SA deployment as illustrated in Figure 3-3. This additional step permits outstations, not just the master, to enforce the roles and privileges of users.

Each user has an Update Key, which may or may not be configured at a given outstation depending on whether that user is intended to have access to the outstation. In the example, Alice's Update Key is configured at three outstations, while Bob's is configured at two and Donald's is configured at only one of the outstations. (There is also a default Update Key – black in the diagram – configured to identify the master to each outstation). A user cannot perform operations on an outstation that does not have that user's Update Key installed. This is true *even if the user gains access to the field network* and tries to interfere between the master and the outstation.

To provide additional security, utilities could choose to have the users' Update Keys installed on security tokens carried by each user, rather than store them in the master. In that case, if the master was compromised, the attacker would acquire only the default Update Keys. The attacker would therefore only be able to perform operations that the default user was given access to do. This could mean, for instance, that the attacker could read data but not perform controls because the default user was not permitted to send control operations.

If an outstation was compromised, the attacker could pretend to be whichever users were configured for that outstation, plus the outstation itself. This risk could be mitigated by having each user use a different Update Key for each outstation, but that would add to the number of keys and complexity.

The primary advantage of this scenario over the previous scenarios is to be able to distinguish between users at an outstation.

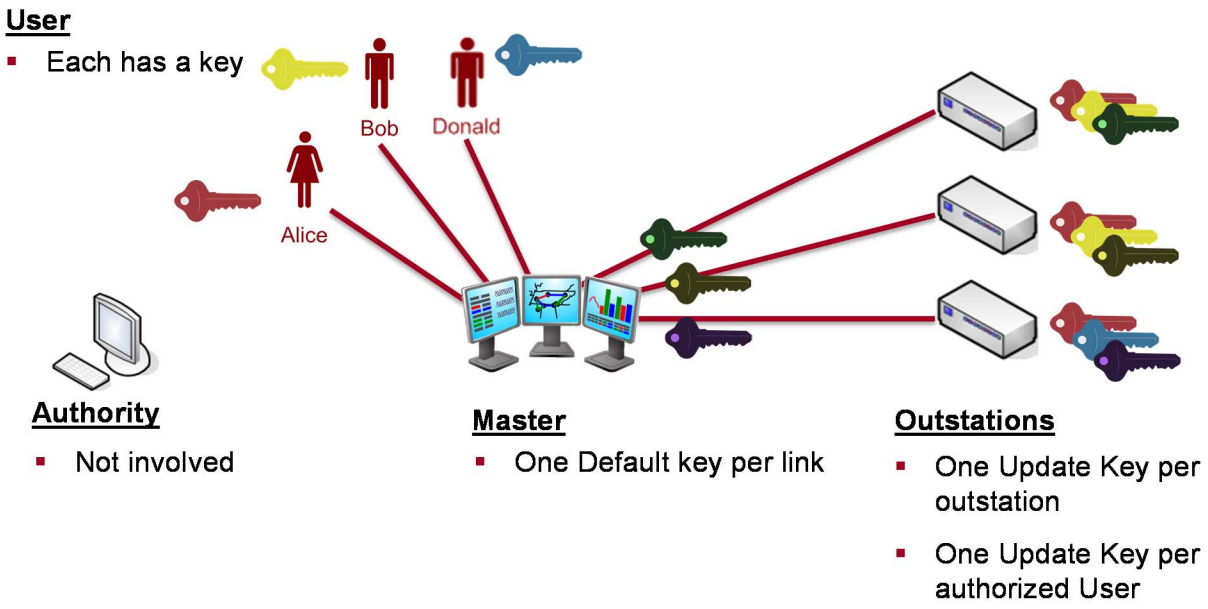

Figure 3-3
Multi-User, Pre-shared Keys Scenario

3.4 Multiple Users, Downloaded Keys, Symmetric Cryptography

As discussed in the previous example, if a utility defines user-specific keys, it significantly increases the amount of pre-configuration required to deploy a DNP3-SA system. The intended solution to this problem is to add a DNP3 authority to the system, and permit Update Keys to be remotely downloaded as illustrated in Figure 3-4 and Figure 3-5.

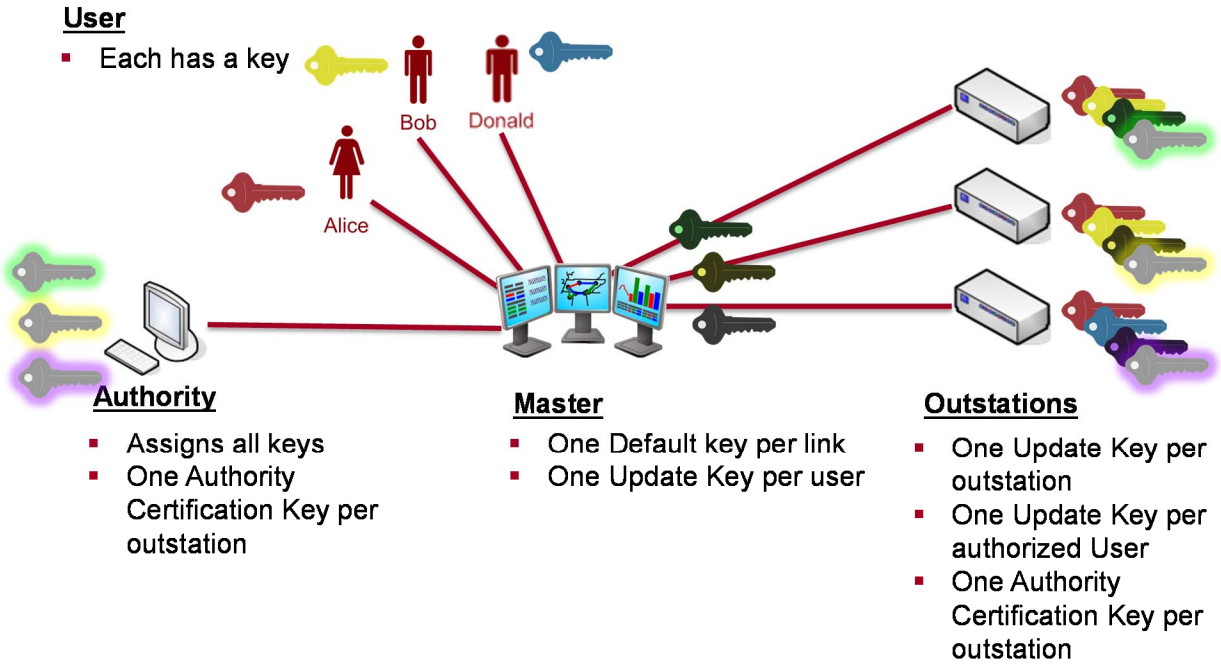

Figure 3-4
Multi-User, Downloaded Keys, Symmetric Scenario – Total Keys

The benefits of this scenario may not be immediately apparent. The total number of keys definitely increases, as shown in Figure 3-4. Now there is an additional Authority Certification Key configured at each outstation, shared between the authority and the outstation (the three "glowing" keys in the diagram).

However, this step actually simplifies the process. The addition of these extra Authority Certification Keys means the Update Keys do not need to be pre-configured at the outstation. The authority can remotely download the default keys to the master and can remotely download the users' keys to the outstations through the master. Figure 3-5 shows how few keys then need to be pre-configured: one per outstation and one per user. Even the user's Update Keys are generated by the central authority as with all the others.

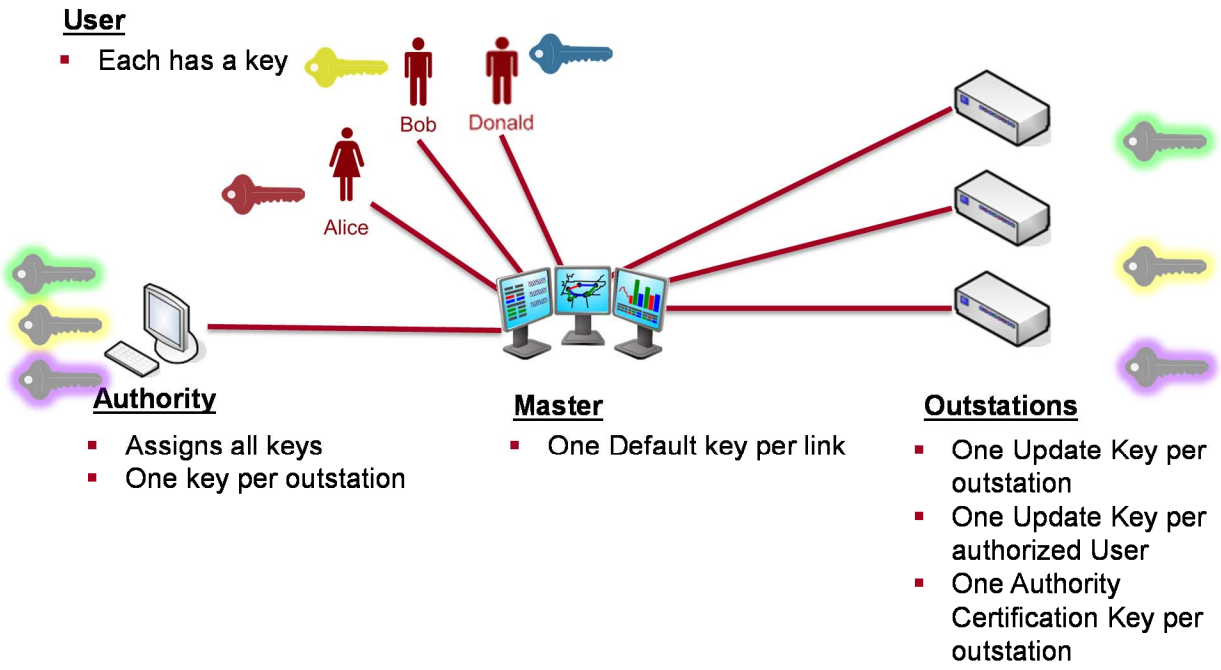

Figure 3-5
Multi-User, Downloaded Keys, Symmetric Scenario – Pre-Configured Keys Only

In these scenarios, an attacker that compromises an outstation can impersonate the outstation or any user that was given access to that outstation, as in previous scenarios. However, with remote key downloading, it is possible to quickly change all those keys very soon after the attack is detected.

There are therefore three advantages to the practice of remotely downloading Update Keys:

- It greatly reduces the cost of traveling to remote sites when key employees leave the organization or when keys are compromised
- It reduces the total number of keys that must be pre-configured, especially for multi-user systems
- It increases the speed with which a utility can react to an attack

3.5 Multiple Users, Downloaded Keys, Asymmetric Cryptography

Using asymmetric cryptography, it is possible to reduce the vulnerability of the DNP3-SA system and reduce the amount of pre-configuration, as illustrated in Figure 3-6. Using asymmetric cryptography, each person or device has two keys:

- a **private key** that must be kept secret, used for digitally signing messages (keys in boxes in the diagram)
- a **public key** that anyone is permitted to see, that is used for authenticating messages (keys not in boxes in diagram) or encrypting keys for that user.

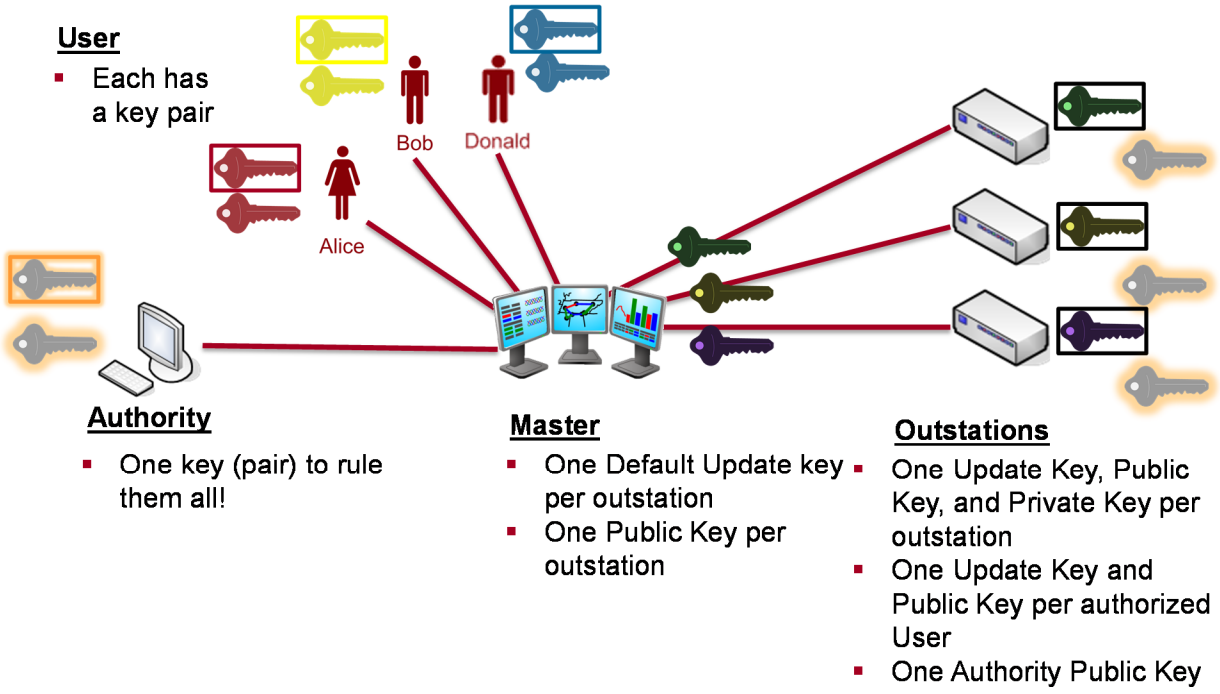

Figure 3-6
Multi-user, Downloaded Keys, Asymmetric Cryptography Scenario

In this scenario, the multiple Authority Certification Keys configured at the outstations in the symmetric scenarios are replaced by a single Authority Public Key ("glowing" in the diagram). This reduces the number of keys managed and improves security. As long as the authority's private key is kept absolutely secret, it does not matter who sees the authority's public key; the mathematics of asymmetric cryptography ensures that an attacker cannot use this key to impersonate the authority.

As shown in Figure 3-6, each outstation must have its own private key configured and kept secret, with the corresponding public key installed at the master. It may be difficult to keep the outstation's private key safe from attack at a remote site. However, this situation is still more secure than in the symmetric scenarios, for the following reasons:

- If the outstation is compromised, the attacker can only impersonate that single outstation in the process of changing Update Keys because that is the only private key on the outstation.
- The attacker cannot impersonate the authority because the outstation only holds the single public key of the authority, as already discussed.
- The attacker cannot impersonate any user to another outstation because the outstation only holds the public key of each user, which was downloaded to the outstation by the authority and master, possibly in the form of a certificate. These keys are shown beside the users in the diagram because they are not pre-configured, but they are eventually downloaded.
- All the downloaded symmetric Update Keys can be changed immediately through remote download, as in the symmetric case. Once the Update Keys are changed, the attacker cannot pretend to be a user or a master.

Therefore, the main difference between the symmetric and asymmetric multi-user cases consists of how much damage an attacker can do between the time an attack on an outstation is detected and when the keys can be completely changed on the system. Using symmetric cryptography, the attacker can change Update Keys on other devices during this time, while using asymmetric cryptography, the attacker is prevented from doing so.

The impact of a disgruntled employee leaving the organization varies in both symmetric and asymmetric cases depending on how the keys of users are managed. Ideally these user keys are kept on secure tokens that are only inserted in the master when the user is logged in. This would ensure that an attacker at the master would only have access to the default keys. As noted previously, having only the default keys may deny an attacker the ability to operate controls and perform other critical operations.

4
DEPLOYMENT OF DNP3-SA IN A SECURE CONTEXT

This section describes some external factors affecting the deployment of DNP3-SA.

4.1 NERC CIP Requirements

A question that many utilities ask is "Where does DNP3-SA fit with respect to the NERC CIP Standards?" First, at the time this document is being written, the mandate of NERC applies only in the bulk electrical system (i.e. transmission) so that distribution networks, where many DNP3 deployments are found, are not affected by the NERC CIP standards by definition.

The argument has also been made that DNP3 is not a "routable protocol" and therefore does not need to be secured. While this is true of DNP3 over serial links, this is certainly not true of DNP3 over IP, because IP by definition is a routable protocol. There is some debate on how this distinction is applied when DNP3 is transferred from an IP network to a serial or radio network.

Specific areas where the use of DNP3-SA may support a utility's efforts to meet the requirements outlined in the NERC CIP standards are primarily focused around NERC CIP-005-5, R1.3 and R1.5. In both cases, these requirements are applied to the Electronic Access Points (EAPs), which are not necessarily the point where DNP3 would be applied. However the capabilities of the devices employed to meet these requirements may be enhanced by the implementation of DNP3-SA within the SCADA traffic that traverses them. DNP3-SA may also serve as a compensating measure employed if the inability to directly meet the requirement is addressed within a Technical Feasibility Exception (TFE).

4.2 SCADA vs Remote Interactive Access

NERC CIP-005-5, R2.1, R2.2, and R2.3 define requirements for "Interactive Remote Access to BES Cyber Systems." The typical position regarding these requirements is that they apply to cases such as remote access for engineering or maintenance activities (human-to-machine) involving the need to login to the devices and do not apply to SCADA communications (machine-to-machine) where DNP3, and DNP3-SA are utilized.

4.3 Patching and Updates

Due to the heavy investment in testing and validation, periodic software updates have not been prevalent within the operational context of the traditional utility control system deployment model. In this model, software patches and updates are typically applied infrequently and involve a lengthy planning process. Unfortunately, cyber-security vulnerabilities are found within commercial computing platforms on a daily basis, and addressing such vulnerabilities in a short enough time period to avoid attacks challenges this status quo.

The goal of the DNP3 Users Group is to provide backward compatibility when updates are made to the DNP3 standards; however this is not always possible when dealing with cyber security vulnerabilities. To remain effective, system and device software associated with the support of DNP3-SA functionality may require regular patching and updates. The DNP3 Users Group has issued an Application Note on this issue that is available to both members and non-members. [4]

It is recommended that products that support secure remote download of software or firmware be utilized.

4.4 What to Log and When

Logging in the classic sense of security is not a requirement of implementing DNP3-SA and is outside the scope of the DNP3 standards. Although not a specific requirement, logging is an extremely important part of the overall security of a utility control system deployment. Section 7.4.1 of IEEE Std 1815-2012 recommends that, at a minimum, the following be logged:

- all successful and unsuccessful authentications
- all successful and unsuccessful key exchanges

It is also recommended that the logs contain:

- the time
- the DNP3 address
- the affected user
- the entire DNP3/DNP3-SA message

4.5 Encryption and Where to Do It

As noted earlier in this document, DNP3-SA does not provide encryption of normal DNP3 traffic and does not address confidentiality except when downloading cryptographic keys. It is recommended in cases where messages must traverse insecure networks, such as the Internet, that Transport Layer Security (TLS) be utilized in conjunction with DNP3-SA to provide both authentication and encryption. In cases where TLS is utilized in conjunction with DNP3-SA, implementers must adhere to the requirements contained within IEC 62351-3 [5] for the use of TLS within a power control system:

- Must use TLS 1.0 or higher
- Must use TLS_RSA_WITH_AES_128_SHA (mandatory suite for TLS v1.2)
- Must renegotiate TLS keys in approximately same time as Session Keys
- Must use a MAC (TLS states this is optional)
- Must support up to four certificate authorities
- Must support TLS certificates of up to 8192 bytes, keys 1024 bits or bigger
- Must support ability to accept either any certificate from a CA or specific individual certificates
- Must check for revocation of certificates every 12 hours by default
- Must terminate connections if revoked, but not if expired

One recent change to the IEC 62351-3 standard is the ability to utilize NULL encryption. Previous versions of the standard required that devices reject NULL encryption but the newest version drops this requirement. When NULL encryption is utilized for a connection, TLS authenticates and provides integrity checks but it does not encrypt the message. This feature may be useful to some utilities for debugging activities associated with commissioning or maintenance of a control system. Without the ability to invoke NULL encryption, utilities may

not be able to utilize testing and maintenance tools such as a SCADA protocol test set. The use of NULL encryption has not been addressed within the DNP3-SA specification.

4.6 Multi-Factor Authentication

The most secure authentication methods involve two or more of the following factors:

- **Something you have** –e.g., a debit card
- **Something you know** –e.g., a personal information number
- **Something you are** –e.g., a signature or a fingerprint

DNP3-SA, like most other cryptographic protocols (e.g., TLS or IPSec) is primarily based on a single "something you know" factor – namely, each end of the communications must use the correct set of keys to communicate. To reduce the risk of depending on this single factor, the master periodically changes the Session Keys using the Update Keys.

One way to add a second factor to DNP3 authentication would be to implement multiple users and have them carry their keys on security tokens as described in sections 2 and 3 of this report. This is most often done with asymmetric cryptography and certificates, but it could also be implemented using symmetric cryptography. Users would not be able to log on to the system or perform secure operations without these tokens, creating a "something you have" authentication factor.

Some utilities already have a two-factor system in place: for instance, at some utilities users carry a token that generates a different number depending on the time of day, and this number must be entered to log into a system. DNP3-SA has not yet been tested with such a system, but it could conceivably be used for access to the master, the DNP3 authority, the certificate authority, or any combination of these systems.

4.7 Denial of Service Attacks

Denial-of-Service attacks are a significant concern to utilities when addressing the security of their automation and control systems. These types of attacks are difficult to defend at the device level. To perform its job or participate in a protocol, a device must spend some finite amount of time processing messages of unknown origin, if for no other reason than to authenticate them. It cannot simply stop processing messages, because this is the attacker's desired goal. Therefore no matter how well-designed the device or the protocol, it is always possible for an attacker to transmit enough messages at a device that the device will be overwhelmed. An informed attacker who understands the mechanics of a particular protocol can furthermore tailor attacks to target specific aspects of the protocol such as session initiation, and in doing solimit, or prohibit, the device's ability to service legitimate users.

Improvements were made in DNP3-SAv5 to address some specific denial-of-service attacks including the requirement that the challenger cease to transmit error messages after a configurable number of failures. Effective denial-of-service protection however cannot be implemented solely at the device level. Utilities' deployment plans should provide for intermediate devices, such as a firewall or intrusion detection system (IDS), which can intervene in a denial-of-service attack by filtering or other mechanisms.

4.8 Intrusion Detection

An IDS is a device or software application that monitors a network or system for anomalous activity or policy violations. Two basic detection techniques are typically employed within IDS; statistical anomaly-based and signature-based. An anomaly-based IDS system first establishes a baseline to define the normal or expected behavior of the system. The IDS then monitors network traffic or system activity and compares it against this baseline to detect significant deviations, or anomalies, from the baseline. A signature-based IDS utilizes a database of defined signatures or attributes of known malicious activity. It then monitors network traffic or system activity and compares it against this database to detect potential anomalies.

IDS technology can be deployed at the network level or host level within a system. In many cases, both types are distributed throughout the system to provide adequate coverage. The use of DNP3-SA mechanisms may provide additional support for a utility IDS deployment by augmenting the IDS monitoring with additional statistics and error messages generated within the end devices.

Firewalls supporting deep packet inspection capabilities can also be utilized external to the end devices to provide additional detection capabilities. These devices are available that support, to some extent, parsing of the DNP3 and DNP3-SA traffic and typically provide either passive (e.g., logging) or active (e.g., blocking) responses to detected anomalies.

Utilities should, at a minimum, define a profile of the DNP3 and DNP3-SA operations that could be expected to be valid within the context of the design of the automation or control system. The byproduct of such a profile yields a list of DNP3 and DNP3-SA operations (such as a warm restart command) that should not be expected and can be actively monitored within the system to detect potentially malicious activity.

4.9 Supply Chain Issues

One important aspect of supporting a successful DNP3-SA deployment is the relationship and effective communications between the utility and its vendors. Important areas that should be discussed with vendors to articulate the utility's needs include:

- The agreement to remove or reset default passwords
- The agreement that there will be no back-door passwords
- The development of a secured mechanism for the vendor to protect and pre-install keys if required by the utility

5
TRICKY BITS OF THE SPECIFICATION

This section provides extra explanation of some concepts within the DNP3-SA standard that may be difficult for implementers to understand. Utilities should ensure their vendors are familiar with the challenges arising from these features. They are discussed here at a high level so that utilities will be able to understand the issues if disputes arise between implementers.

5.1 Challenge Sequence Numbers

The challenge sequence number (CSQ) field in DNP3-SA messages is used to identify when new random challenge data is being included in the MAC calculation. The expected CSQ value may be incremented by either the master or the outstation depending on what other features are enabled in the DNP3 protocol, such as aggressive mode or unsolicited responses. Therefore there are a fairly complex set of rules associated with the calculation of CSQs. The following is a simplified summary of these rules. Each device:

1. Sets CSQ to zero on startup
2. Increments CSQ each time it transmits a Challenge
3. Sets the CSQ of each Reply to that of the Challenge
4. Increments CSQ each time it sends a Reply / Aggressive Mode Request
5. Increments CSQ each time it receives a valid Aggressive Mode Request
6. Wraps the CSQ around after 32 bits
7. Uses the same CSQ for all Users, ***one in each direction***

5.2 Aggressive Mode

Aggressive mode is an option that must be supported by any DNP3-SA device. Enabling this option causes MACs to be appended to the critical DNP3 messages they authenticate. This significantly reduces the number of messages required to perform authentication because there is no need for a separate Challenge and Reply message, as shown in Figure 5-1 compared to Figure 1-3 on page 1-4.

However, before using Aggressive Mode, each device must ensure that at least one Challenge and Reply message exchange takes place every time the Session Keys are changed. This ensures that the challenge data remains sufficiently unpredictable to protect against replay attacks.

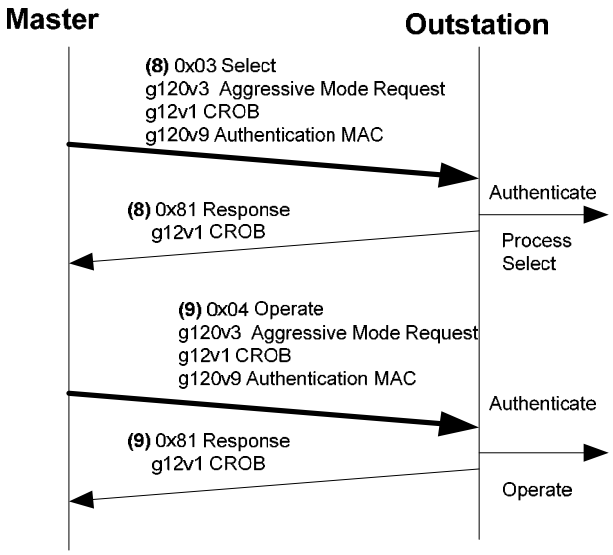

Figure 5-1
Use of Aggressive Mode, Extracted from IEEE Std 1815-2012

5.3 Aggressive Mode Confirmations

When an outstation transmits event (change) data in normal DNP3, it sets the CON (confirm) bit so the master is required to send a Confirm message for the event data and the outstation then knows it can release the buffer containing the events.

Using DNP3-SA it is possible, although not required, for an outstation to require event Confirm messages from the master to be authenticated. If aggressive mode is enabled, the MAC for the Confirm message must therefore be contained within the Confirm message itself. For this to work properly when using aggressive mode, the outstation must "piggy back" the random Challenge data on the original event message, as illustrated in Figure 5-2.

5.4 Unsolicited Responses

Unsolicited Responses is a feature of normal DNP3 that permits an outstation to transmit data whenever changes occur rather than always transmitting data in response to a request from the master. This feature can greatly reduce the latency of the system in detecting important changes such as breaker trips.

Unsolicited responses complicate the implementation of DNP3-SA because they can affect the calculation of CSQs. It is possible for messages from the master and outstation to pass in transit, both incrementing the CSQ. There are therefore several rules defined in the specification to avoid conflicts, the most important of which is that the master and outstation must maintain separate sets of challenge data to be used for normal Responses and Unsolicited Responses.

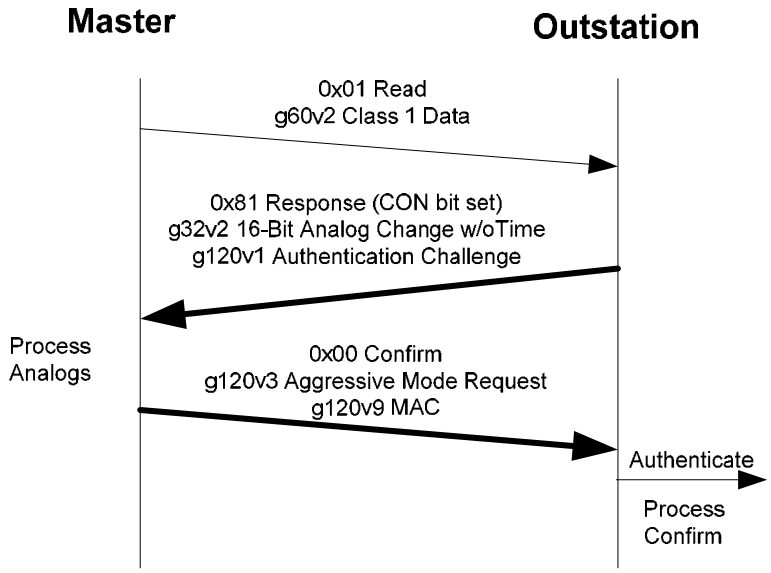

Figure 5-2
Using Confirms in Aggressive Mode, Extracted from IEEE Std 1815-2012

6
IMPLEMENTING SECURITY

No matter how much effort a utility places on developing a security architecture or the implementation of DNP3-SA within an automation or control system, the effectiveness of these efforts can be less than desirable if proper precautions are not taken to ensure the protection of key information. If key information within a DNP3-SA system is compromised, it may not be possible to maintain the integrity of the data protected by that key information.

6.1 Keeping Key Material Secret

FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* [7], identifies best practices for protecting key information. Four levels of security for key information protection are defined within the standard with Security Level 1 being the lowest and Security Level 4 being the highest. Requirements identified within the definition of the Security Levels will influence a utility implementing DNP3-SA in several ways including equipment and device requirements, security architecture development, and key processes and procedures developed to support the effective operation of the system. It is recommended that at a minimum, DNP3-SA implementations comply with the requirements of Security Level 2 or higher.

An important characteristic of utility SCADA systems is that a majority of outstation devices are located in remote and unattended facilities making them specifically vulnerable to physical access. Utilities must take measures to ensure that key information is not available within the outstation devices to potential attackers by:

- encrypting keys that are stored in configuration files
- eliminating the possibility of displaying keys within the outstation
- providing that key changes can only be made by users with correct roles

6.2 Transporting Key Material

In cases where key information needs to be transported to and from DNP3 outstation devices, the key must be transported in a secure manner. This transportation can be done physically using an electronic device such as a secure USB drive that holds the key information or it can also be done electronically over a computer network. In either case, Utilities implementing DNP3-SA should follow guidance outlined in NIST SP 800-57, *Recommendation for Key Management* [8] when handling and transporting key information.

6.3 Security Training

While technical solutions are essential for effective protection of key information, organizational culture is also an important component. For this reason, security training for all personnel involved at any point in the lifecycle of the automation or control system should be required. Security training should address:

- policies, processes, and procedures for all aspects of key management
- roles and responsibilities for all personnel

7
INTERACTION WITH NON-SECURE DNP3 SYSTEMS

This section describes how devices implementing DNP3-SA are expected to interact with devices that do not implement DNP3-SA. It describes several example scenarios and how the protocol is expected to behave in each case. The word "will" in the following scenarios indicates behavior that is specified to occur in the DNP3 standard. "Shall" is not used because this document is not the standard and is not specifying the standard behavior, just describing it. The word "should" indicates behavior that is not in the standard but is expected good practice in typical devices.

7.1 Non-Secure Master, Secure Outstation

In this case, any critical function performed by a non-secure master (such as a control operation, see Table 2-1) will cause a secure outstation to send an Authentication Response fragment (Function Code 0x83) containing an Authentication Challenge (g120v1) object. This will happen even though no Session Keys have been established.

The master will not recognize this function code and should log or raise an alarm indicating it has detected an incompatibility between its configuration and that of the outstation.

The outstation will timeout when it does not receive an Authentication Request fragment (Function Code 0x20) containing an Authentication Reply (g120v2) object. It will not retransmit, and will not respond to the control operation.

Even if the master has not correctly alarmed the unrecognized function code 0x83, it will time out waiting for the response to the control operation, and the operator should see the control failure.

7.2 Secure Master, Non-Secure Outstation

A secure master will attempt to initialize Session Keys before performing any secure operation, using an Authentication Request fragment (Function Code 0x20) and an Authentication Key Status Request (g120v4).

The non-secure outstation will not recognize the function code or the object and will send a Response containing the appropriate Internal Indication error bits set.

The master should log or alarm that it has detected a configuration error because of the Internal Indication errors.

7.3 Gateway Upstream Secure, Downstream Non-Secure

A gateway acting as an intermediary between a secure master and a non-secure outstation will request that a master properly authenticate all critical operations before the gateway sends corresponding messages to the outstation. For example, if the master performs a control on the gateway but does not supply the correct MAC, the gateway will never send the outstation the corresponding control operation.

The master may also optionally require that the gateway properly authenticate itself when the gateway forwards data transmitted by the outstation to the master.

7.4 Gateway Upstream Non-Secure, Downstream Secure

In this case, the gateway should (must) assume that the non-secure commands it receives from the master are authentic and authorized, and always send them to the outstation. The outstation will require that the gateway authenticate every critical message transmitted. (Mandatory critical functions are listed in Table 2-1; the outstation may require additional functions be considered critical.) The gateway may optionally require that the outstation authenticate the data the outstation is transmitting.

The gateway will always appear as a single user to the outstation, unless it can distinguish between multiple upstream masters by some other method, such as address, port or protocol used by the master. In that case, the gateway will authenticate with the outstation as a different user for each master.

8
MIGRATION FROM SAV2 TO SAV5

As noted earlier in this report, there have been two released version of DNP3-SA; the initial version 2 release (SAv2) included in IEEE Std 1815-2010 and updated version 5 release (SAv5) included in IEEE Std 1815-2012. The main differences are that SAv2 supported only pre-shared symmetric keys while SAv5 also supports remotely changing keys by symmetric or asymmetric methods. SAv5 also corrected problems identified in the SAv2 release. This section is based on the Application Note from the DNP Users Group that was issued with the release of SAv5. [9]

8.1 Multiple Versions Simultaneously

The DNP Users Group recommends that SAv2 not be deployed in new installations. Although SAv2 has been deprecated within the 2012 edition of IEEE Std 1815, utilities may be faced with the need to continue to support existing outstation devices that support only SAv2. For this reason, DNP3 master stations should support both SAv2 and SAv5 and allow this to be configured on a per device level. In cases where both the master and outstation support both SAv2 and SAv5, SAv5 should be utilized.

8.2 New Algorithms

The evolution of security threats is one of the most challenging aspects of developing an automation or control system security architecture. Advances in both technology and the skill sets of potential adversaries necessitates the need to evolve to newer and more secure algorithms when those existing ones are known to be weak or broken and vulnerable to attack. The update to SAv5 addressed this need and added cryptographic algorithms not supported in SAv2 as follows:

- It changes the minimum length of an HMAC to 8 octets instead of 4.
- It makes SHA-256 a mandatory hash algorithm, and the default.
- It makes it a requirement that the use of SHA-1 can be disabled by configuration.
- It changes the mandatory TLS cipher suite to one supported by TLS version 1.2.
- It clarifies which pseudo-random number algorithm should be used.
- It optionally permits the use of the AES-256 Key Wrap algorithm.
- It optionally permits the use of the AES-GMAC algorithm for calculating MACs. Using this algorithm places some additional rules on the rest of the protocol.

All SAv2 algorithms are still permitted in SAv5. A SAv5 device is not required to support the mandatory SAv2 cipher suite.

8.3 Unsolicited Responses

Unsolicited responses from a DNP3 outstation need to be secured in addition to securing requests and solicited responses. SAv2 did not adequately address all the possible interactions between solicited and unsolicited SA messages passing each other in transit. To address these interactions, SAv5 changes the calculation of Challenge Sequence Numbers (CSQ) and specifies that separate Challenge Data must be used for solicited and unsolicited communications.

This is the primary incompatibility between SAv2 and SAv5. The two versions will not calculate the correct expected CSQ in some cases, causing incorrect authentication failures.

8.4 Role-Based Access and Authorization Control

While SAv2 provided mechanisms by which the outstation could conclusively identify an individual user (not just the device) that transmits any DNP3 message, it did not specify the required mechanisms by which the outstation could apply role-based access control. SAv5 permits outstations to limit access to certain functions, either based on the specific user's identity or based on the role assigned to the user. This role-based access control is only possible if one of the optional methods for remotely changing pre-shared keys is implemented.

8.5 Statistics

A significant tool in a utility's ability to detect a potential attack is the ability to identify patterns of behavior that might be suspect. SAv5 added objects and procedures for maintaining and reporting statistics about the operation of the Secure Authentication protocol (e.g., the number of authentication failures). A SAv2 master station will not recognize the statistics objects and will likely discard these objects. *A compatibility problem arises if it also discards any other data in the same message.*

8.6 Error Messages

To reduce the impact of specific types of denial-of-service attacks, SAv5 specifies fewer cases than SAv2 in which the device sends an error message. SAv5 devices now only send error messages for configuration errors, not operational errors such as timeouts or unexpected messages. In these cases, the device simply discards the incoming message silently.

8.7 Other Differences

Other differences between SAv2 and SAv5 which affect their compatibility include:

- *Critical Confirms* - SAv2 specified that outstations wishing to consider Application Confirms from the master as critical can send a Challenge Object to request that the Confirm be sent in Aggressive Mode. SAv5 clarifies a few specific situations that the devices must handle to make this possible.
- *Restarts* - SAv2 did not adequately specify what should happen when an outstation or master restarts, particularly regarding the initialization of Session Keys. SAv5 specifies that the master shall not require the initial Null Unsolicited Response be critical, and that the Master shall reset Session Keys before performing any other actions upon detecting an outstation restart, but should not do so more often than a configured number of times per Key Change Interval. SAv5 also clarifies that a Challenge/Reply sequence must take place after every Session Key change before Aggressive Mode can be used, not just after a restart.

9
REFERENCES

1. IEEE Power and Energy Society, “IEEE Std 1815-2012, IEEE Standard for Electric Power System Communications - Distributed Network Protocol,” Institute for Electrical and Electronic Engineers (IEEE), New York, 2012.
2. International Electrotechnical Commission, “IEC 62351-5 ed2.0, Data and Communications Security - Part 5: Security for IEC 60870-5 and derivatives,” IEC, Geneva, Switzerland, 2013.
3. International Electrotechnical Commission, “IEC 62351-8 ed 1.0, Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control,” IEC, Geneva, Switzerland, 2011.
4. DNP Technical Commitee, “DNP3 Application Note AN2012-001, Managing DNP3 Secure Authentication Updates,” DNP Users Group, 2012.
5. International Electrotechnical Commission, “IEC 62351-3 ed1.0, Data and Communications Security - Part 3: Communication Network and System Security - Profiles including TCP/IP,” IEC, Geneva, Switzerland, 2014.
6. DNP Technical Committee, “Application Note AN2013-004b, Validating of Incoming DNP3 Data,” DNP Users Group, 2014.
7. U.S. Dept. of Commerce National Institute of Standards and Technology, “FIPS PUB 140-2: Security Requirements for Cryptographic Modules,” U.S. Government Printing Office, Washington, 2001.
8. U.S. Dept. of Commerce National Institute of Standards and Technology, “NIST SP 800-57: Recommendation for Key Management,” U.S. Government Printing Office, Washington, D.C., 2012.
9. DNP Technical Committee, “Further Information Regarding the Release of DNP3 Secure Authentication Version 5 (SAv5),” DNP Users Group, 2011.

10
GLOSSARY

The following terms are used in this document.

AES	Advanced Encryption Standard
aggressive mode	An option in DNP3-SA in which a device appends a MAC to a critical function message rather than waiting for a challenge and sending a reply
API	Application Programming Interface
Asymmetric cryptography	A class of cryptographic algorithms in which the keys used at either end of the communication are different
Authority Certification Key	The cryptographic key shared between a DNP3 authority and an outstation to download Update Keys using symmetric cryptography
BES	Bulk Electric System
CA	Certificate Authority
certificate	An electronically signed document attesting that a particular entity (or person) is associated with a particular asymmetric public key
certificate authority	An entity which signs cryptographic certificates
challenge	A DNP3-SA message sent to request authentication, containing random data to be used in the calculations which follow.
CIP	Critical Infrastructure Protection standard
cipher	A cryptographic algorithm used to encrypt or decrypt a block of data
cipher suite	A set of cryptographic algorithms used to achieve a particular purpose
CRC	Cyclic Redundancy Check
critical function	A DNP3 message or messages that the receiver of the message requires to be authenticated
CRL	Certificate Revocation List
CSQ	Challenge Sequence Number
CSR	Certificate Signing Request
DKMP	DNP3 Key Management Protocol. Not yet a standard; developed as part of the 2014 DNP3-SA Interoperability Demonstration
DNP3	Distributed Network Protocol. Sometimes abbreviated just DNP.
DNP3 authority	An entity which manages DNP3 users, roles and keys
DNP3-SA	DNP3 Secure Authentication (any version)
DNP3-SAv2	DNP3 Secure Authentication Version 2
DNP3-SAv5	DNP3 Secure Authentication Version 5
EAP	Electronic Access Point
FIPS	(U.S.) Federal Information Processing Standard
GMAC	Galois Message Authentication Code
hash	A cryptographic algorithm used to check the integrity of a message
HMAC	Hashed Message Authentication Code
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standards Organization
key	A block of data used in cryptographic algorithms, part or all of which is kept secret
MAC	Message Authentication Code
master	The controlling end of a DNP3 communication link
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology (U.S. Dept. of Commerce)
OCSP	Online Certificate Status Protocol
outstation	The controlled end of a DNP3 communication link
pre-shared key	A key that must be physically configured at both ends of a communication link instead of being remotely downloaded. Also called pre-configured.
private key	The key in asymmetric cryptography that must be kept secret. Mathematically linked to a public key.
PUB	Publication
public key	The key in asymmetric cryptography that may be seen by anyone. Mathematically linked to a private key.
public key cryptography	Another term for asymmetric cryptography
reply	A DNP3-SA message containing a Message Authentication Code
revoke	Action taken to notify entities in a security system that a certificate is no longer valid
role	An attribute of a user that indicates the user has a particular set of privileges
SAv2	DNP3 Secure Authentication Version 2 (abbreviated)
SAv5	DNP3 Secure Authentication Version 5 (abbreviated)
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Lifecycle
Session Key	The lowest level of cryptographic keys used in DNP3-SA, which are changed periodically
SHA	Secure Hash Algorithm
SP	Special Publication
Symmetric cryptography	A class of cryptographic algorithms in which the key used at either end of the communication must be the same key
TCP	Transmission Control Protocol
TFE	Technical Feasibility Exception
TLS	Transport Layer Security
UDP	User Datagram Protocol
Update Key	The cryptographic keys used in DNP3-SA to change and encrypt Session Keys
USB	Universal Serial Bus
user	A term used in DNP3-SA to indicate a person operating an outstation from a master station
VPN	Virtual Private Network

A
THE 2014 DNP3-SA INTEROPERABILITY DEMONSTRATION

This Appendix describes the demonstration organized by EPRI in 2014 to illustrate interoperability between products implementing DNP3-SA according to IEEE Std 1815.

A.1 History and Background

A.1.1 Value to the Industry

DNP3 is the most widely used utility communications protocol in North America. Over 75% of power utilities have reported using it as part of their SCADA, substation automation or feeder automation projects. Originally released in 1994, DNP3 has been continuously updated over the years by an active community of suppliers, users and integrators within the DNP Users Group.

Unfortunately, DNP3 as originally defined was not secure. Like most utility protocols developed at the time, it was designed to be highly resistant to noise and other communications failures found on power system feeders, but had no protection against deliberate cyber-attacks. In today's security context this omission was critical because DNP3 is frequently used by utilities over vulnerable communications links, such as unencrypted radio systems. It is sometimes carried over third-party wide area networks whose owners may not implement adequate security. And even communications links that were traditionally thought to be secure, such as leased lines, have been shown to be vulnerable.

Therefore, ensuring that DNP3 communications are secure is an important goal for the power industry. Furthermore, because of DNP3's popularity, it is a project that can provide a huge benefit through relatively modest investment in a single technology.

A.1.2 Goals and Deliverables

This demonstration project encourages the adoption of security for DNP3 by illustrating that several implementations of DNP3-SA (IEEE Std 1815) are available and that the implementations are compatible with each other. From the report on this demonstration, utilities can know which suppliers participated and begin specifying projects to evaluate the technology.

To meet these goals, this project had the deliverables:

- This report
- Spreadsheet containing the list of scenarios tested and the results
- Logs of the scenarios tested
- The DNP3 Key Management Protocol (DKMP) specification

A.1.3 Previous Accomplishments

EPRI sponsored the following successful deliverables regarding the development of DNP3-SA

- Development of the specification itself and its related standards: IEC 62351-5 and IEC 60870-5-7
- Review and adoption of the specification with the DNP User's Group, the Smart Grid Interoperability Panel, the IEC and the IEEE
- Preparation and review of compliance test procedures for DNP3-SA

A.2 Demonstration Objectives

This section describes the objectives of the demonstration.

A.2.1 Demonstrate the Basic Functions of DNP3-SA

The first objective of the demonstration was to show that the basic functions of DNP3-SAcould be successfully performed among products from multiple vendors. The functions chosen for demonstration are described in the *Test Scenarios* section of this report.

A.2.2 Demonstrate Co-Existing DNP3-SAv2, DNP3-SAv5 and Non-Secure Environments

The second objective was to demonstrate that utilities will be able to migrate their systems from non-secure to secure DNP3, and from version 2 to version 5 of the standard. The team illustrated this capability by performing scenarios in which:

- Several existing gateway devices were able to convert from one method of DNP3 communications to the other while performing a secure control operation. All the gateways participating in the demonstration performed this conversion the same way: by terminating one DNP3 connection, storing data changes in some type of intermediate database, and initiating another DNP3 connection to another device.
- The three different DNP3 communications methods co-existed without interference on the same Ethernet local area network. This capability is possible because DNP3 communications makes use of protocol layering through the Internet protocol suite.

A.2.3 Demonstrate a Complete System Including Key Management

The third objective of the demonstration was to show that interoperable products are available for all the types of components found in a typical utility deployment of DNP3-SA. The desired components included:

- Master stations
- Outstations (sometimes known as Intelligent Electronic Devices, or IEDs)
- Gateways (devices serving as both masters and outstations)
- Test Sets
- DNP3 Authorities, as described by the DNP3-SA standard
- Certificate Authorities

Demonstrating key management (e.g., remotely adding, deleting or changing the role of a user and changing Update Keys) was considered to be an important part of this objective because:

- This capability is the main difference between SAv2 and SAv5.
- Using these functions may provide significant cost reduction for utilities. By implementing remote key management, utilities would not need to send personnel to perhaps hundreds or thousands of sites to change keys when utility employees joined or left the organization.
- The interfaces between master stations, DNP3 authorities and certificate authorities have not yet been standardized. Therefore the demonstration was an excellent opportunity to investigate and develop possible technologies for implementing these information exchanges.

To focus on this objective, a sub-group consisting of the vendors who were interested in performing key management was defined at the beginning of the project. The key management team met separately from the main group to address the technical challenges associated with achieving this goal.

A.2.4 Identify Areas that May Need Clarification in the Specification

The fourth objective of the demonstration was to help the DNP Users Group improve the specification by providing feedback on sections that might be vague or confusing, leading to lack of interoperability. A few items were found and this report will be submitted to the DNP Users Group to help them improve the standard.

A.3 Demonstration Schedule

The demonstration was planned and executed following the schedule shown in Table A-1. The primary milestones were the following items, highlighted in yellow in the table:

- The **Kickoff** web conference took place on June 4, 2014
- The **Vendor "Plug-fest"** to execute the full set of test scenarios and determine any technical problems took place from September 15-17, 2014 in the EPRI Substation Lab in Knoxville, Tennessee. Utilities did not attend this part of the demonstration.
- The **EPRI DNP3 Technology Transfer Workshop** [hereafter referred to as the workshop], took place on November 6, 2014. The agenda of the workshop included:
  - Training on the DNP3-SA protocol
  - Explanation and history of the demonstration project
  - Demonstration of a subset of the set of test scenarios (15 out of 192)

The workshop was preceded by two "dry runs" of the scenarios that were to be demonstrated at the workshop; one online and the other on-site at EPRI.

The original dates for the plug-fest and the workshop were August 26-28 and October 28 respectively. These were rescheduled as indicated in Table A-1 because it was found that key participants could not attend on the original dates. It was extremely fortunate that the other participants were able to reschedule and the effort of these participants to do so was very much appreciated by EPRI.

As shown in Table A-1 and noted in the "*Demonstration Objectives*" section of this report, there were two streams of meetings that took place to organize the demonstration:

- Meetings including all the participants. The full team meetings focused primarily on selection and definition of test scenarios and the logistics for performing them. These meetings are identified in the "*Meeting*" column and highlighted in blue in Table A-1.
- Additional meetings involving only those who were participating in the key management scenarios of the test. The key management meetings discussed scenarios and logistics but also discussed the design and implementation of key management messaging between the master and DNP3 authority, and the use of external certificates for managing keys and users. This process is described in detail in the "Development of the DNP3 Key Management Protocol (DKMP)" section of this report. The key management meetings are identified in the "Meeting" column and highlighted in pink in Table A-1.

Table A-1
Demonstration Schedule of Events

Date	Meeting	Type	Accomplishments
2014-06-04	Kickoff	online	Reviewed first draft of scenarios and network diagram
2014-07-01	Key management	online	Draft of XML messages submitted for review
2014-07-09	Key management	online	Chose TLS for authentication, reviewed messages
2014-07-16	Key management	online	Started DKMP document, discussed technology choices
2014-07-22	Key management	online	Chose technology: XML messages directly on TLS
2014-07-29	Key management	online	Reviewed the DKMP document
2014-08-05	Key management	online	Identified steps for user key distribution
2014-08-07	Full team	online	Defined connectivity matrix, reviewed scenarios
2014-08-18	Full team	online	Defined IP addresses, key formats, finalized scenarios
2014-08-19	Key management	online	First messages sent between master and authority
2014-08-20	Key management	online	Identified objectives for using external certificates
2014-08-29	Full team	online	Rescheduled plug-fest to 2014-09-15, discussed logistics
2014-09-04	Full team	online	Defined key sizes, algorithms, scenario steps, lab diagram
2014-09-04	Key management	online	Defined steps for using external certificates
2014-09-11	Full team	online	Reviewed vendor-specific scenario list, defined plug-fest process, rescheduled workshop to 2014-11-06
2014-09-15 to 2014-09-17	Vendor "Plug-fest"	in person	90% completion of test scenarios!
2014-10-20	Full team	online	Summarized plug-fest, defined initial workshop scenario list, set up VPN for remote duplication of scenarios
2014-10-24	Full team	online	Establishing communications, scheduled dry runs
2014-10-27	Key management	online	Full key management functionality testing begins
2014-10-28	Full team	online	Duplicating scenarios online, troubleshooting
2014-10-29	Key management	online	Successfully performed symmetric key change
2014-11-03	Online dry run	online	Troubleshooting of logistics and configuration; no technical barriers to executing scenarios successfully
2014-11-05	On-site dry run	in person	Successful execution of all scenarios but took a long time due to logistics
2014-11-06	EPRI DNP3 Technology Transfer Workshop	in person	Successful demonstration well within allotted time!

A.4 Test Scenarios

This section describes the interoperability test scenarios chosen by the demonstration participants. The scenarios chosen were grouped into the following categories according to the objectives identified for the demonstration:

- **Protocol Scenarios** – demonstrated basic functionality of DNP3-SA
- **Topology Scenarios** – demonstrated coexistence and migration of DNP3-SAv5, DNP3-SAv2 and non-secure DNP3
- **Key Management Scenarios** – demonstrated the ability to remotely add, delete or change the roles and Update Keys of users

A.4.1 Protocol Scenarios

The basic protocol functions demonstrated by the participants included the following items:

- Establish and periodically renew Session Keys
- Authenticate messages using Challenge/Reply and Aggressive Mode, including invalid authentication
- Authenticate messages in both directions
- Recover from communications and device failures
- Authenticate over TCP/IP, serial, and TLS profiles of DNP3
- Count and retrieve communications statistics

A.4.2 Topology Scenarios

The participants demonstrated the following scenarios illustrating conversion of a control output command between versions of DNP3:

- DNP3-SA version 2 to version 5 and vice versa
- Serial DNP3-SAv5 to IP-based DNP3-SAv5 and vice versa

A.4.3 Key Management Scenarios

The key management functions demonstrated by the participants included the following items:

- Identify new users to outstations and download keys for these users to the outstations
- Change user roles and verify the corresponding change in user privileges
  - Perform these tasks using both symmetric and asymmetric cryptography
  - Create and use standard IEC 62351-8 certificates to perform these tasks

A.4.4 Scenario List

There were 41 functional scenarios chosen, each of which could be performed by several different DNP3-SA devices, as shown in Table A-2.

Each of these functional scenarios was broken down into a number of device-specific scenarios demonstrating communications between a particular set of participants, as shown in Table A-3. The numbering convention for scenarios is as follows:

- Letter indicating the category of scenario: “T” for topology scenarios, “P” for protocol scenarios, or “K” for key management scenarios
- Scenario number within the category
- A dash “-“
- Number indicating the version of the protocol used: “2” or “5”
- A dot “.”
- Device-specific scenario number

The device columns of the spreadsheet indicate which role the device performed in the scenario:

- “M” indicates the device acted as a master station
- “O” indicates the device acted as an outstation
- “G” indicates the device acted as a gateway, i.e. as an outstation in one direction and a master in another direction
- “T” indicates the device acted as a test set to monitor the scenario and generate a log

The complete list was defined in a spreadsheet and totaled 192 device-specific scenarios. The results of the plug-fest and workshop are discussed in section A-7 of this report.

Table A-2
List of Functional Scenarios

No.	Category	Demonstration Scenario	Demo Nov 6	Version	ESCRYPT	Triangle authority	Red Hat	Schneider ClearSCA	Triangle DTM	Cooper Visual T&D	OSI Monarch	Schneider SAGE RTU	SUBNET Sub Server	NovaTech Orion LX	Cooper SMP / SG	ASE2000	Schneider SCADAPa	Cooper SMP (O)	Gridco DGC	Triangle Test Harnes	OSI OSIRIS
T1-5	Topology	Non-secure DNP3 master operates control thru gateway to secure IED		SAv5						M		G	G		O			O		O	
T2-5	Topology	Secure DNP3 master operates control thru gateway to non-secure IED		SAv5					M	M	M								O	G	
T3-5	Topology	Secure DNP3 master operates control thru gateway to secure IED		SAv5					M	M	M				G	M			O		O
T4-5	Topology	Use of Secure Authentication over TLS		SAv5					M						O						
T5-5	Topology	Serial DNP3 master operates secure control on IP-based outstation		SAv5						M											O
T6-5	Topology	IP-based DNP3 master (Cooper) operates secure control on serial outsta	Yes	SAv5						M								O			
T7-5	Topology	Secure DNP3 master operates control directly to secure IED		SAv5							M							O			
T8-5	Topology	Gateway converts between SAv5 and SAv2		SAv5							M				G	M	O				
T3-2	Topology	Secure DNP3 master operates control thru gateway to secure IED		SAv2				M	M			G					O	O			
P1-5	Protocol	Initialize Session Keys		SAv5					M	M	M		M	M	G	T			O		O
P2-5	Protocol	Periodically refresh Session Keys		SAv5					M	M	M		M	M	G	T			O		O
P3-5	Protocol	Challenge / Reply of critical operation (e.g. control)		SAv5					M	M	M		M	M	G	T			O		O
P4-5	Protocol	Reject invalid Challenge / Reply		SAv5											O	M			O		O
P5-5	Protocol	Aggressive Mode Request of critical operation (e.g. control)		SAv5					M	M	M		M	M	G	T			O		O
P6-5	Protocol	Reject invalid Aggressive Mode Request		SAv5											O	M			O		O
P7-5	Protocol	Recover from loss of communication network		SAv5					M	M	M		M	M	G	T			O		O
P8-5	Protocol	Recover from loss of outstation		SAv5					M	M	M		M	M	G	T			O		O
P9-5	Protocol	Recover from loss of master		SAv5					M	M	M		M	M	G	T			O		O
P10-5	Protocol	Read security statistics		SAv5					M							O			O		
P11-5	Protocol	Authenticate data from outstation		SAv5							M										O
P1-2	Protocol	Initialize Session Keys		SAv2				M	M			G					O	O			
P2-2	Protocol	Periodically refresh Session Keys		SAv2				M	M			G					O	O			
P3-2	Protocol	Challenge / Reply of critical operation (e.g. control)		SAv2				M	M			G					O	O			
P4-2	Protocol	Reject invalid Challenge / Reply		SAv2					M			O					O	O			
P5-2	Protocol	Aggressive Mode Request of critical operation (e.g. control)		SAv2				M	M			G					O	O			
P6-2	Protocol	Reject invalid Aggressive Mode Request		SAv2					M			O					O	O			
P7-2	Protocol	Recover from loss of communication network		SAv2				M	M			G					O	O			
P8-2	Protocol	Recover from loss of outstation		SAv2				M	M			G					O	O			
P9-2	Protocol	Recover from loss of master		SAv2				M	M			G					O	O			
P11-2	Protocol	Authenticate data from outstation		SAv2				?	?			?					?	?			
K1-5	Key Mgmt	Manually change pre-shared Update Keys		SAv5						M	M								O		O
K2-5	Key Mgmt	Remotely change Update Keys using symmetric cryptography		SAv5	A	A			M											O	
K3-5	Key Mgmt	Remotely change Update Keys using asymmetric (Public Key) cryptography		SAv5	A	A			M											O	
K4-5	Key Mgmt	Remotely change Update Keys using asymmetric (Public Key) certificates		SAv5	A	A	CA		M											O	
K6-5	Key Mgmt	Reject operation because user does not have necessary privileges		SAv5					M		M									O	
K7-5	Key Mgmt	Reject operation because user's privileges have expired		SAv5	A				M											O	
K8-5	Key Mgmt	Reject operation because user has been deleted		SAv5	A				M											O	
K1-2	Key Mgmt	Manually change pre-shared Update Keys		SAv2				M	M			G					O	O			
K5-2	Key Mgmt	Reject operation because user does not have necessary privileges		SAv2				M	M			G					O				

Table A-3
Example of Device-Specific Scenarios for Functional Scenario "P1 – Initialize Session Keys"

No.	Category	Demonstration Scenario	Demo Nov 6	Version	ESCRYPT	Triangle authority	Red Hat	Schneider ClearSCAD	Triangle DTM	Cooper VisuaLT&D	OSI Monarch	Schneider SAGE RTU	SUBNET Sub Server	NovaTech Orion LX	Cooper SMP / SG	ASE2000	Schneider SCADAPack	Cooper SMP (Q)	Gridco DGC	Triangle Test Harness	OSI OSIRIS
P1-5	**Protocol**	**Initialize Session Keys**		**SAv5**					**M**	**M**	**M**		**M**	**M**	**G**	**T**			**O**		**O**
P1-5.1	Protocol	Triangle Initializes Session Keys with Cooper		SAv5					M						O	T					
P1-5.2	Protocol	Cooper Initializes Session Keys with Cooper		SAv5						M					O	T					
P1-5.3	Protocol	OSI Initializes Session Keys with Cooper		SAv5							M				O	T					
P1-5.4	Protocol	Subnet initializes Session Keys with Gridco		SAv5									M			T			O		
P1-5.5	Protocol	Subnet initializes Session Keys with ASE		SAv5									M			O					
P1-5.6	Protocol	Subnet initializes Session Keys with OSI		SAv5									M			T					O
P1-5.7	Protocol	NovaTech initializes Session Keys with Gridco		SAv5										M		T			O		
P1-5.8	Protocol	NovaTech initializes Session Keys with ASE		SAv5										M		O					
P1-5.9	Protocol	NovaTech initializes Session Keys with OSI		SAv5										M		T					O
P1-5.10	Protocol	Cooper initializes Session Keys with Gridco		SAv5											M	T			O		
P1-5.11	Protocol	Cooper initializes Session Keys with ASE		SAv5											M	O					
P1-5.12	Protocol	Cooper initializes Session Keys with OSI		SAv5											M	T					O
P1-5.13	Protocol	ASE initializes Session Keys with Cooper		SAv5											O	M					
P1-2	**Protocol**	**Initialize Session Keys**		**SAv2**				**M**	**M**			**G**					**O**	**O**			
P1-2.1	Protocol	Schneider master initializes Session Keys with Schneider RTU		SAv2				M				O									
P1-2.2	Protocol	Triangle initializes Session Keys with Schneider		SAv2					M			O									
P1-2.3	Protocol	Schneider RTU initializes Session Keys with Schneider IED		SAv2								M					O				
P1-2.4	Protocol	Schneider RTU initializes Session Keys with Cooper		SAv2								M						O			
P1-2.5	Protocol	Cooper SMP/SG initializes Session Keys with Cooper SMP4		SAv2								M						O			

A.5 Test Equipment and Layout

This section describes the equipment and layout of the interoperability demo.

A.5.1 Participating Vendors and Products

Table A-4 lists the participating vendors, their products, and the roles the products played in the demo. The notation "Gateway" means that the product acted as both a master and outstation simultaneously.

Table A-4
Participating Vendors and Products

Vendor	Product	Role in Demonstration			Version	
		Master	Outstn	Other	SAv5	SAv2
ESCRYPT	CycurKEYS			DNP3 Authority and CA	Yes	
Red Hat	Identity Management (IdM) in Red Hat Enterprise Linux			Certificate Authority (CA)	Yes	
Triangle MicroWorks, Inc.	DNP3 Key Manager			DNP3 Authority and CA	Yes	
	Distributed Test Manager	Yes		Test Set	Yes	Yes
	Communication Protocol Test Harness	Yes	Yes	Test Set	Yes	Yes
Schneider Electric	SCADA Expert ClearSCADA	Yes				Yes
	SCADAPack E Smart RTU	Yes	Yes	Gateway		Yes
	SAGE RTU	Yes	Yes	Gateway		Yes
Eaton's Cooper Power Systems	Visual T&D	Yes			Yes	
	SMP/SG	Yes	Yes	Gateway	Yes	Yes
	SMP4		Yes		Yes	Yes
Open Systems International (OSI)	monarch™	Yes			Yes	
	OSI Remote Information System (OSIRIS™) RTU		Yes		Yes	
Applied Systems Engineering, Inc.	ASE 2000 version 2 Test Set	Yes	Yes	Test Set	Yes	Yes
SUBNET Solutions Inc.	SubSTATION Server™ 2	Yes	Yes*	Gateway	Yes	
NovaTech, LLC	OrionLX Automation Platform	Yes	Yes*	Gateway	Yes	
Gridco Systems	Distributed Grid Controller (DGC™)		Yes		Yes	

* = Non-secure DNP3 only.

These are only the roles the products played in the demonstration; they may have additional capabilities. For instance, the SMP4, the OSIRIS, and DGC were also capable of acting as gateways, but did not do so in this demonstration.

A.5.2 Connectivity

Figure A-1 illustrates the logical connections between the products participating in the demonstration. Colors indicate the type of communications used, as described in the legend.

Table A-5 illustrates the individual connections made between the products participating in the demo, including the Internet Protocol Version 4 (IPv4) addresses and DNP3 addresses of each device.

The "Type" column and row in Table A-5 indicate the role played by the device: "M" for master, "O" for outstation, "A" for authority and "CA" for certificate authority. Colors and text in each cell indicate that a connection was made, and what type the connection was.

Physically, all products were connected to a single switch in a star-shaped configuration using twisted pair CAT5 cabling, and configured on a single IPv4 subnet. The test sets were connected to the "mirror ports" of the switch in order to monitor communications.

There were two terminal servers used to demonstrate the ability to communication DNP3-SA over a mixed serial and IP-based network. These terminal servers were Perle STS4 D Secure Terminal Servers. The one serially connected to the Cooper Visual T&D was configured to automatically create an IP connection with the Gridco device. The one serially connected to the Gridco device was configured to accept an IP connection from the Cooper Visual T&D.

All equipment was located in EPRI's Substation Laboratory in Knoxville, Tennessee.

A.5.3 Users

To simplify the testing and improve chances of interoperability, all devices were configured to use the single default user for all operations. The exceptions to this rule were the key management scenarios, in which several different users with different roles were created and deleted.

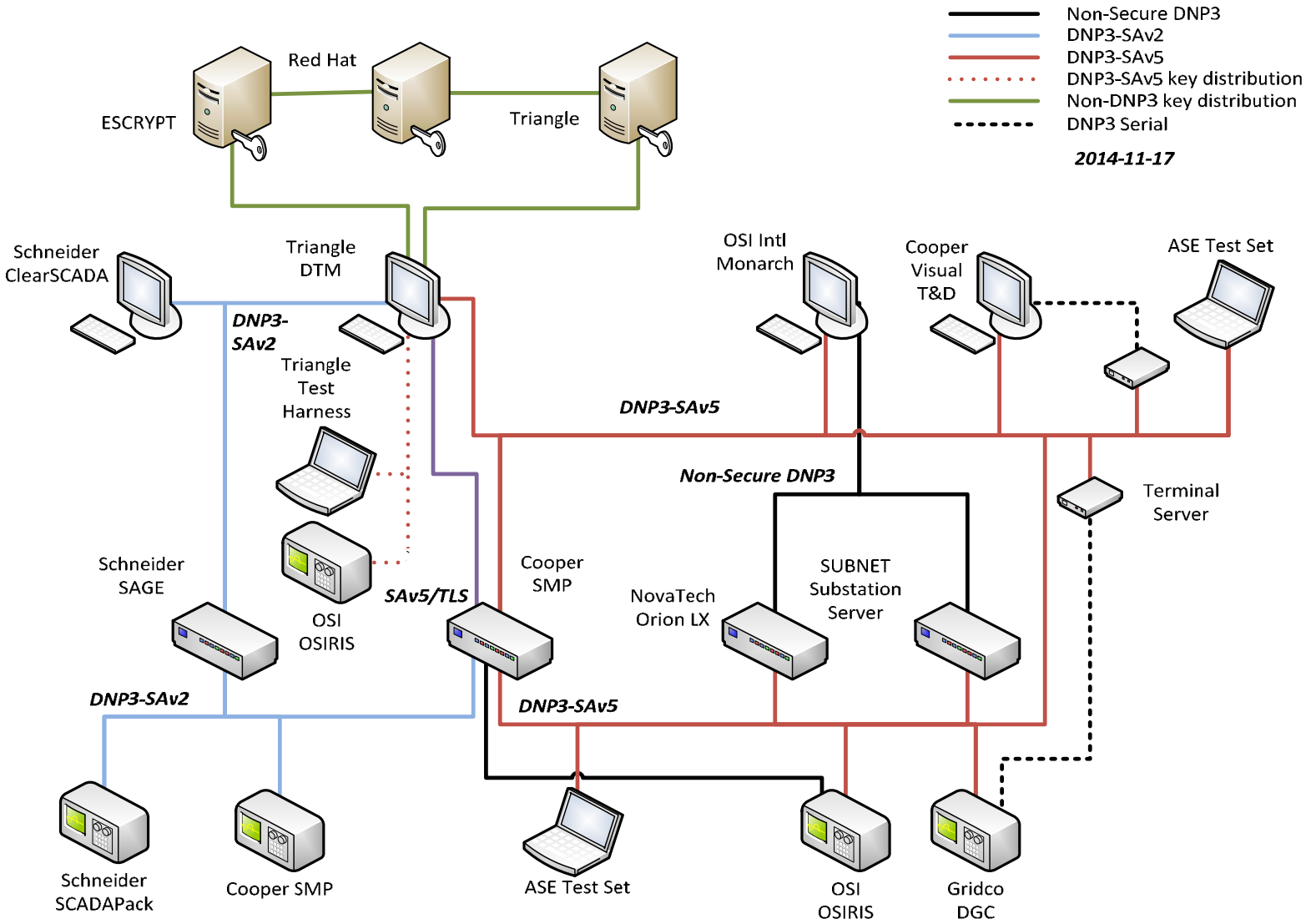

Figure A-1
Logical Network Diagram

Table A-5
Detailed Connectivity

Participants	No. of IPs	Master or Single IP Address	Outstation IP Address	DNP Address (same as last byte of IP)		ESCRYPT	Red Hat	Schneider ClearSCADA	Triangle DTM	Cooper Visual T&D	OSI Monarch	Schneider SCADAPack	SUBNET Sub Server	NovaTech Orion LX	Cooper SMP / SG	ASE2000	Schneider SAGE	Cooper SMP (O)	Gridco DGC	Triangle Test Harness	OSI OSIRIS	Terminal Server
					Type	A	CA	M	M	M	M	O	O	O	O	O	O	O	O	O	O	O
ESCRYPT	1	10.1.1.50 / 18		n/a	A		YES		DKMP													
Red Hat	1	10.1.1.51 / 18		n/a	CA																	
Schneider ClearSCADA	1	10.1.1.52 / 18		52	M							SAv2										
Triangle DTM	1	10.1.1.53 / 18		53	M							SAv2			SAv5				SAv5	SAv5	SAv5	
Cooper Visual T&D	1	10.1.1.54 / 18		54	M										SAv5				Thru TERM			SERIAL
OSI Monarch	1	10.1.1.55 / 18		55	M								DNP3	DNP3	SAv5				SAv5		SAv5	
Schneider SCADAPack	2	10.1.1.56 / 18	10.1.1.57 / 18	56/57	M												SAv2	SAv2				
SUBNET Sub Server	2	10.1.1.58 / 18	10.1.1.59 / 18	58/59	M											SAv5			SAv5		SAv5	
NovaTech Orion LX	2	10.1.1.60 / 18	10.1.1.61 / 18	60/61	M											SAv5			SAv5		SAv5	
Cooper SMP / SG	2	10.1.1.62 / 18	10.1.1.63 / 18	62/63	M											SAv5	SAv2	SAv2	SAv5		SAv5	
ASE2000	2	10.1.1.64 / 18	10.1.1.65 / 18	64/65	M														SAv5			
Schneider SAGE RTU	1		10.1.1.66 / 18	66	O																	
Cooper SMP (O)	1		10.1.1.67 / 18	67	O																	
Gridco DGC	1		10.1.1.68 / 18	68, 70 (serial)	O																	SERIAL
Triangle Test Harness	1		10.1.1.69 / 18	69	O																	
OSI OSIRIS (two outstatio	1		10.1.1.71 / 18	71	O																	
Terminal Servers (two of	2	10.1.1.72 / 18	10.1.1.73 / 18	72, 73	O																	

A.5.4 Conventions

Again to simplify the logistics of the test, the following agreements were made among the participants in the demo:

- All DNP3 addresses would be the same as the last byte of the IP address of the device.
- The Update Keys used to establish Session Keys would be derived from the IP address of the outstation on which the test operation was to be performed. This is NOT a recommended security practice, and in a real system would introduce a significant vulnerability. The agreement was made to avoid wasting time during the plug-fest and workshop trying to determine which Update Key was being used.
- All control operations would be LATCHed so the state change would remain visible after the operation was performed.
- All control operations would be select-before-operate. However, many direct operate commands were also successfully performed just in preparation for testing.

A.5.5 Test Equipment and Software

As indicated in Table A-4, there were two different DNP3 test sets used. These test sets were also used to monitor the messages between other devices and capture logs of the test scenarios.

The open-source tool Wireshark was used on some of the Windows-based products i to verify connectivity early in the testing. Wireshark is able to parse DNP3, although it does not provide detailed parsing of SA.

Most of the products supported some sort of DNP3 tracing tool on their own user interfaces. These were also used to capture logs of some of the test scenarios.

A.5.6 Software Implementations

The vendors were not queried on what software they used to implement DNP3. However, it is estimated that there were at least four unique implementations of DNP3 participating.

A.5.7 Presentation Methods

To present a subset of the test scenarios at the workshop the following method was used, as illustrated in Figure A-2:

- Two laptops were connected to projectors in the conference room.
  1. One laptop projected versions of Figure A-1 with arrows overlaid to illustrate which scenario was being demonstrated.
  2. One laptop at the podium of the conference room used EPRI's virtual private network software to access a workstation in the EPRI Substation Laboratory using Remote Desktop Protocol (RDP).
- The workstation in the laboratory then used a variety of methods to connect to the devices participating in the demonstration, and project these interfaces on the screen for the workshop participants:
  1. Secure Shell (SSH)
  2. Web Browser

3. Remote Desktop Protocol (RDP)
4. Custom vendor-specific configuration software

- The podium laptop accessing the workstation also ran GoToMeeting web collaboration software. Vendors both inside the conference room and at remote sites were therefore able to operate their own device interfaces as if they were using the podium laptop. To speed up the demonstrations, some vendors stepped to the podium to use that laptop directly.

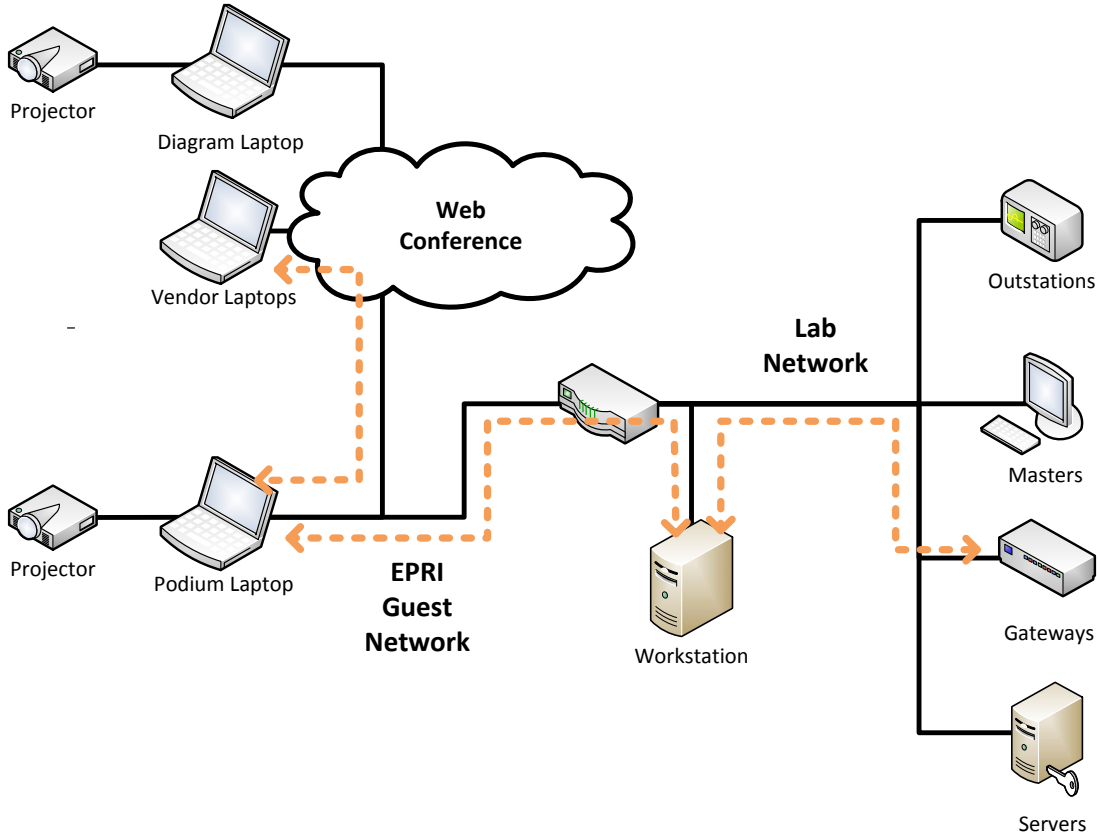

Figure A-2
Presentation of Scenarios at the Workshop

A.6 Development of the DNP3 Key Management Protocol (DKMP)

This section describes the activities of the demonstration members who participated in the key management and user management portions of the testing, as described in the "Key Management Scenarios" section of this report.

As noted in the "*Demonstration Objectives*" section, implementing these scenarios was challenging. Although the DNP3-SA specification describes what information should be exchanged between a DNP3 master and a DNP3 authority, it does not describe the format or technology to be used for these messages, since they would be outside of the normal scope of DNP3 between the master and outstation.

These decisions had to be discussed, agreed upon, and documented by the participants before they could proceed with implementation. The resulting protocol has been named the "DNP3 Key Management Protocol" or DKMP.

A.6.1 Vendor Participation

The participants in the key management portion of the demonstration and the roles their products played are listed in Table A-6.

Table A-6
Participants in Key Management Scenarios

Participant	Product	Role			
		Master	Out-station	Authority	Certificate Authority
Red Hat	Identity Management (IdM) in Red Hat Enterprise Linux				Yes
ESCRYPT	CycurKEYS			Yes	Yes
Triangle MicroWorks, Inc.	DNP3 Key Manager			Yes	Yes
	Distributed Test Manager	Yes			
	Communication Protocol Test Harness		Yes		
Open Systems International (OSI)	OSI Remote Information System (OSIRIS™) RTU		Yes		

The following items should be noted about the participants and products in the demonstration:

- The OSIRIS product was not initially participating in the key management part of the demonstration. OSI announced at the end of September that they could have a compatible product ready to test for the plug-fest, and were able to do so. The OSIRIS RTU acted as an outstation in the key management scenarios.
- Red Hat has not yet determined which products will include the modifications they made to their software to support IEC 62351-8 certificate extensions. As shown in Table A-6, the most likely candidate is Identity Management (IdM) in Red Hat Enterprise Linux. However, the capability may also be deployed in the Red Hat Certificate System (RHCS) product.

A.6.2 Major Design Decisions

The participants needed to make a number of design decisions when developing DKMP. They are summarized as follows:

- **Client vs. Server.** It was debated which component should act as a TLS client as opposed to a TLS server. It was decided that the DNP3 Authority would act as a TLS server, since the master is requesting the services of the Authority in managing user credentials.
- **Authentication.** There was a possible choice between using TLS for authentication between the master and authority, and using application layer messaging to perform authentication. The team agreed to use TLS to not add complexity to the application layer. They further agreed to use the mutual authentication option of TLS to ensure both ends of the link were provided with an equal level of security. Standard TLS certificate handling was used for the authentication.

- **Messaging Technology.** The team agreed to use XML messaging directly on TLS. Several application layer candidates were considered, including AMQP, SOAP and some form of REST messaging using web services. However, the team found that there was no benefit from adding additional layers of protocol in this case. XML was seen as useful for two reasons: it provides both a human-readable means of documenting the protocol, and a built-in encoding format. A small header was added to identify the length of each XML message. In tribute to the well-known start octets of the DNP3 protocol, the value 0x05640564 is used as an identifier for the DKMP header.
- **Update Key Generation and Distribution**. The DNP3-SA specification in the IEEE 1815-2012 standard does not specify which component should generate the user public and private key pair when using asymmetric cryptography. It also does not specify how the keys should travel between the components, although it suggests some alternatives (see Note 3 of clause 7.6.1.4.10 of IEEE Std 1815-2012). Basing their decisions on security best practices, the key management team developed the procedure shown in Figure A-3 and described below:
  1. The DNP3 Authority generates the user's key pair and stores the public key internally.
  2. The DNP3 Authority stores the user's private key on a secure USB token that the user takes into possession. To avoid cost and complexity for this demonstration, an actual security token was not used and the private key was actually emailed between the participants, simulating a user moving from the DNP3 Authority to the master station. This practice should NEVER be followed in a real system, since it compromises the user's private key.
  3. The operator of the DNP3 Authority submits the public key to the Certificate Authority using a standard (PKCS#10) Certificate Signing Request (CSR). To avoid adding complexity for this demonstration, the CSR was manually entered on the existing Red Hat web interface. The operator of the DNP3 Authority was first authenticated to the web interface using a separately installed certificate generated previously.
  4. The operator of the DNP3 Authority enters additional parameters identified in IEC 62351-8 such as the Role to be assigned to the user.
  5. The Certificate Authority creates a signed certificate for the user and presents it to the operator of the DNP3 Authority, who installs it in the DNP3 Authority.
  6. The DNP3 Authority sends a UserStatusChangeRequest DKMP message to the master station, containing the user's certificate.
  7. The master station forwards the certificate to the outstation in a DNP3-SA User Certificate (g120v8) object as part of the defined DNP3-SA protocol sequence.
  8. The user logs into the master and is authenticated by the master. This authentication would typically use the information on the user's secure token, but not necessarily. The team decided not to restrict the method by which the user authenticates to the master. For the demonstration, the user simply logged into the master using Microsoft Windows login.
  9. At some point the DNP3 Authority submits an UpdateKeyRequest to the master station. The master station could store this UpdateKey until the user logs in, or generate the Update Key itself when needed. An early version of the DKMP specification required the master request the Update Key from the DNP3 Authority whenever the user logged in.

The team decided that this unnecessarily restricted the behavior of the master and the user, and might cause Update Keys to be changed unnecessarily frequently. Therefore the team agreed that such a request message would be considered optional for the master to implement, but required for the DNP3 Authority to implement.

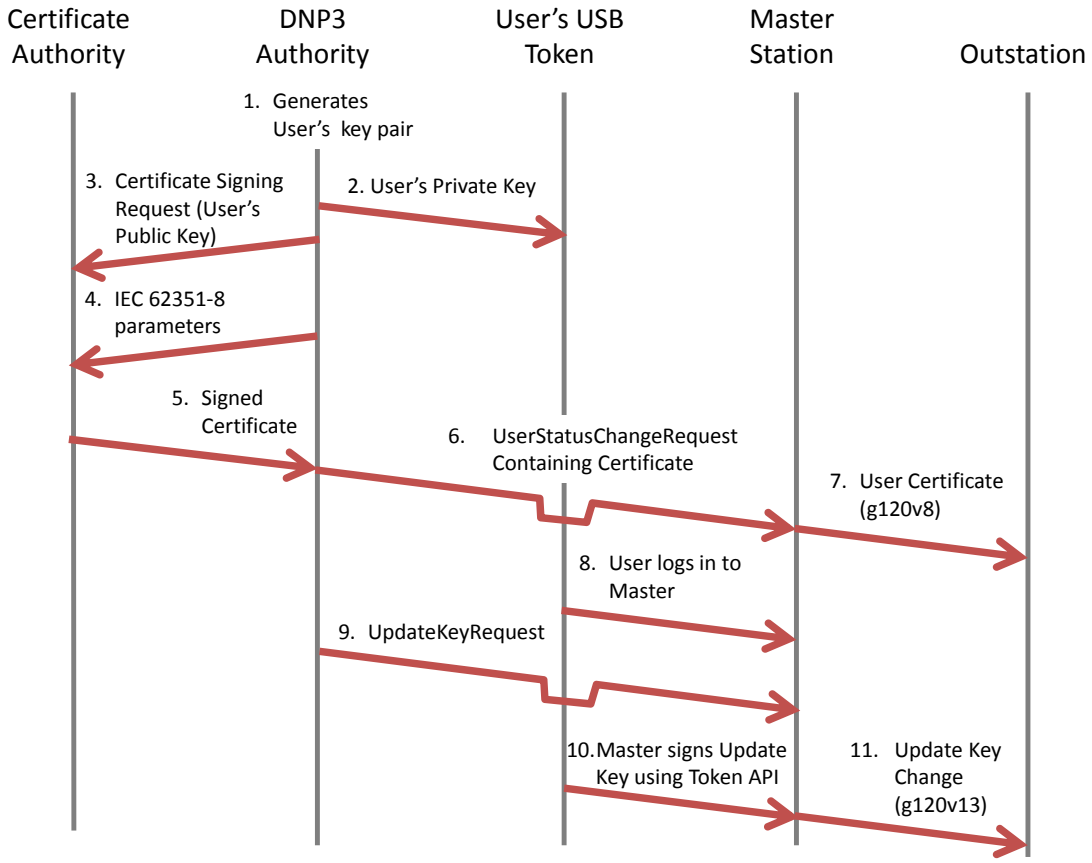

Figure A-3
Update Key Generation and Distribution Sequence – Asymmetric Cryptography

10. Once the master has the new Update Key and the user has logged in, the master uses the secure API on the user's security token to digitally sign the Update Key. For the demonstration, the private key was simply installed as a file on the master because secure tokens could not be implemented in time. In a real system this practice should NEVER be followed since it compromises the user's private key by letting it out of the user's possession.
11. The master sends the signed Update Key to the outstation. The outstation authenticates the master and the new Update Key according to the DNP3-SA protocol, and begins to use the new Update Key.

- **Aggregating Messages.** It was stated by some participants that in systems with a large number of outstations, it would be more efficient to aggregate messages between the DNP3 Authority and the master station; that is, send a single message concerning many outstations rather than sending individual messages for each outstation. However, the team decided not to aggregate messages in this way, for several reasons:

- There was no evidence that bandwidth or processing power between the master and DNP3 authority would be a concern.
- Messages between the master and outstation were already specified in DNP3-SA as individual, non-aggregated messages.
- There were only two outstations participating in the demonstration.
- It was simpler to implement individual messages for the demonstration.

- **Algorithms.** The team chose to use Key Change Method <4>, the default, for demonstrating symmetric key management. The team chose Key Change Method <68> for demonstrating asymmetric key management, but found that the DSA-2048-SHA-256 algorithm for digital signing was not available to more than one participant. The team agreed to continue to use the value <68> but use RSA signatures instead. This is a major concern for the DNP3-SA specification, as discussed in the "Challenges Encountered and Lessons Learned" section of this report.
- **Type of Certificate**. IEC 62351-8 and IEEE Std 1815-2012 define both Attribute Certificate and Identity Certificate formats. For the demonstration, it was to only use Identity Certificates because it was simpler and because using Attribute Certificates would not provide significant additional value.
- **Port Number.** It will be necessary for the DNP Users Group to register a standard TLS/TCP port number for DKMP. For the demonstration, an unused user-defined port was used.
- **Area of Responsibility.** For simplicity, the Area of Responsibility (AOR) text string field of the IEC 62351-8 certificates was fixed for the demonstration as "epridemo". Future demonstrations may wish to test scenarios in which this field varies, to demonstrate additional levels of security enforcement at the outstation.
- **Sequence Number Synchronization.** As discussed in the "Challenges Encountered and Lessons Learned" section of this report, there were concerns about the authority not being able to determine what Status Change Sequence Number would be appropriate to include in each new User Status Change message. It was decided for purposes of the demonstration to use trial and error to determine what sequence number to use, since the outstation will accept any number larger than the last one it received. However, a better mechanism is needed.
- **External Certificates.** As discussed in the "Demonstration Objectives" section of this report, it was a major goal to have multi-vendor participation in all parts of the DNP3-SA communications, including key management. Therefore, the team agreed to implement a scenario in which the Red Hat software provided the certificate which changed the role of a user, the outstations recognized Red Hat as a valid root certificate authority, and the ESCRYPT and Triangle MicroWorks software passed the certificate along. Both ESCRYPT and Triangle MicroWorks software also implemented their own certificate authorities.

A.6.3 Documentation and Standardization of the Protocol

Triangle MicroWorks volunteered to document the DKMP specification, as agreed upon for this demonstration. It is available from EPRI as a separate document from this report.

The participants in the demo agreed to support the standardization of this protocol by the DNP Users Group and IEEE. The participants also signified they understood that the final version of the protocol may differ from that defined for the demonstration.

A.7 Demonstration Results

A.7.1 Completion of Test Scenarios

As listed in Table A-7, there were 192 interoperability test scenarios defined. 162 of these scenarios, or 84%, were completed during the plug-fest, and 15 of them were reproduced for the workshop.

In general, all participants were enthusiastic about the level of success in this demonstration. Most of the time in the lab was spent on the logistics of determining which scenario was being tested and ensuring all participants were prepared for the tests. The numbers show that the tests themselves overwhelmingly succeeded, and usually succeeded the first time they were attempted.

The participants attempted to generate a log of each scenario completed, but this was not always possible, and sometimes it was forgotten. For this reason, the number of tests completed and number of tests logged were not identical. Tests were logged a number of different ways: using a DNP3 test set, using Wireshark, or using debugging tools on the devices themselves.

Table A-7
Scenarios Completed at the Plug-fest

Type	Test Scenarios	Completed		Logged	
		Count	%	Count	%
Total	192	162	84%	155	81%
Topology	34	31	91%	31	91%
Protocol	140	122	87%	115	82%
Key Mgmt	18	9	50%	9	50%
SAv5	132	118	89%	115	87%
SAv2	42	36	86%	32	76%

There were a number of reasons why tests could not be completed:

- The test failed due to an interoperability or implementation problem. These accounted for 11 of the incomplete scenarios. More detail on these problems is provided in the "Challenges Encountered and Lessons Learned" section of this report. All of these problems were resolved by the day of the workshop, although to reduce risk, the corrected scenarios were not included in the list of scenarios demonstrated at the workshop.
- The test was not performed because the vendor was not ready to test. These accounted for 9 of the incomplete scenarios, all of which were in the key management set of tests. It is not surprising that the completion percentage in this area was the lowest, because the entire key management process and the DKMP interface was designed and implemented completely within the time of the demonstration project. One of the most important scenarios – download of a user certificate and changing Update Keys using external certificates and asymmetric cryptography – could not be completed at the plug-fest, but was completed for the first time on the day of the workshop.

- The test was not completed because the participants did not find the time to perform it. These accounted for the remaining 21 of the 30 incomplete tests. Most of these tests were duplicates of scenarios that were performed by other sets of participants. However, one important scenario that was unfortunately never completed was testing DNP3-SA over TLS. That scenario was never tested although all proposed participants were confident that it would work. Another important scenario that was not tested was the ability to authenticate data transmitted by the outstation (as opposed to the master).

A.8 Comparison to the Objectives

The results of the demonstration compared to the objectives are shown in Table A-8.

Table A-8
Evaluation of the Demonstration vs. the Objectives

Objective	Results
Demonstrate the basic functions of DNP3-SA	122 out of 140 device-specific protocol scenarios were successfully tested, including 10 of 11 basic protocol functions identified for the demonstration. The ability to authenticate data transmitted by the outstation was not tested.
Demonstrate co-existing DNP3-SAv2, DNP3-SAv5, and non-secure environments	The participating devices included all three of these groups connected to a single Ethernet switch, with no conflicts detected. 31 out of 34 topology scenarios were successfully tested, illustrating conversion between each of these three groups of implementations.
Demonstrate a complete system including key management	The scenarios tested included implementations in all of the desired categories of devices. Key management was successfully demonstrated from DNP3 authority down to outstation using symmetric cryptography, and from certificate authority to outstation using asymmetric cryptography (although a multi-vendor scenario of the latter only took place on the final workshop day).
Identify areas that may need clarification in the specification	A few clarifications were identified, as noted in the "Recommended Changes to the Standard" section of this report.

A.9 Next Steps

This section suggests next steps that could be made to build on the progress made by this project.

A.9.1 Recommended Changes to the Standard

It is recommended that the DNP Users Group make the following changes to the standard:

- **Clarify the documentation regarding user numbers** so it is clear that the ability to support single-user systems is mandatory and multi-user systems are optional.
- **Clarify the documentation of initialization** so it is clear the responsibility to initialize session keys and respond to challenges takes precedence over other tasks when initializing communications between two devices.
- **Add a method to synchronize status change sequence numbers** between the DNP3 authority and the outstation. According to the present version of the standard, the outstation is required to accept any number larger than the last one it received, but relying on that rule

leads to a trial-and-error process to synchronize sequence numbers if the DNP3 authority loses synchronization.

- **Add a method to remotely and securely identify which users are configured** on a given outstation. In theory, the DNP3 Authority should have this information recorded and not need to acquire it from an external source. However, if the information on the Authority is lost or out of date, it is difficult to determine which users have been added without using the specific configuration tools of each outstation, and even then the information may not be readily available.
- **Re-evaluate the required algorithms** for key management to provide signature options that are more likely to be available than the existing DSA choices.

A.9.2 Recommendations for Future Demonstrations

It is recommended that future demonstrations of this type include:

- **Testing at a utility site.** This demonstration took place under very controlled conditions in the EPRI substation lab. Testing at a utility would be very instructive.
- **More testing of error cases.** The objectives of this demonstration were primarily to show successful interoperability and so there were a minimum of error scenarios defined. Future demonstrations might focus on finding more subtle implementation errors or misunderstandings of the specification.
- **More key management scenarios.** End-to-end multi-vendor interoperability of key management was successfully shown in this demonstration, but not all combinations were tested. It would be useful to illustrate compatibility of the key management solution with corporate infrastructure such as Microsoft Active Directory, RADIUS or Kerberos.
- **Testing over TLS.** This demonstration did not complete the one scenario defined for TLS. Utilities would likely be interested in the results of this scenario.
- **Testing authentication of outstation data.** This scenario was not tested in this demonstration, and would be of interest to utilities.
- **More devices.** Naturally, it would be preferable to have more devices in the demonstration, and for the devices that implemented only SAv2 to also implement SAv5. The participation of more dedicated IEDs (as opposed to gateways) would also help utilities feel comfortable with DNP3-SA as an end-to-end solution.

B
AVOIDING SOFTWARE VULNERABILITIES

Software vulnerabilities introduced during product development activities can be difficult to detect and are often discovered when investigating the root cause of unexpected system or device behavior. This section describes some of the types of software vulnerabilities that have been discovered in DNP3 software and what utilities and vendors can do to mitigate the risk of such vulnerabilities. This section is based on the Application Note on this topic provided by the DNP Users Group [6] .

B.1 Input Validation

As a general principle, all input parameters passed in DNP3 messages should be validated before the software attempts to act on them. Failure to provide for proper input validation within a software application which supports DNP3 and DNP3-SA can lead to vulnerabilities which can affect the reliability of either the master station or outstations within a utility automation or control system. Specific recommendations provided by the DNP Users Group include:

- Parse and validate all incoming data using a “trust nothing” approach before processing it or performing any actions based on the data.
- The code must reflect the functionality of the device; the developer must know the device and what is to be implemented. Validation of object data should be robust and object-dependent; the handling of unexpected/invalid data will need to be device-dependent and well-thought-out (e.g., master requests that do not apply to an outstation’s specific functionality, timestamps that contain invalid values that cannot be converted to a realistic internal time, counter values that decrease, etc.).
- All fields of all data objects should be checked for "reasonable" or valid values (e.g., bits in flag words, values of code fields, etc.).
- Application Programming Interfaces (APIs) should validate all data for applications. Types passed across API boundaries should be as strong as possible to prevent potential integration vulnerabilities.
- Perform testing of boundary conditions, and combinations of boundary conditions. Perform a “reasonableness” test before allocating or consuming resources (e.g., unreasonable number of objects/points).

B.2 Forwarding Error Codes

The error codes produced by lower-level software should be carried up to the highest levels of software and not ignored. Specific recommendations provided by the DNP Users Group in this area include:

- Logging (what is logged, as well as changeable log levels) should be considered as a component of robust handling of error conditions.

B.3 Stopping Processing

Do not continue attempting to process a DNP3 message after the first error is found in the message. Continuing to process a DNP3 message which has induced a system error condition increases the risk of the system of device being vulnerable to a denial-of-service attack. Specific recommendations provided by the DNP Users Group in this area include:

- Stop parsing when a non-recoverable failure (e.g. invalid function code) is encountered, and do not parse any further objects in the fragment.
- Verify that resource allocation has succeeded before attempting to use the resources. It is important to know how to check for the failure; it is not easy in all systems. Failure cases should be handled robustly.

B.4 Memory Management

Check that memory is properly allocated before attempting to use the memory. Specific recommendations provided by the DNP Users Group in this area include:

- Ensure that the parsing/processing of variable-length data, file transfer, etc. is robust in order to avoid accessing out-of-bound memory.
- Consider the removal of debugging artifacts and associated constructs from the production code.
- When discarding messages, all code artifacts should be 'tidied up' (e.g. buffers reset/cleared, variables reset to default values, etc.) so that subsequent processing does not encounter remnants from previous messages.

B.5 Data Format Conversion

Software code that performs the function of converting data from one format to another is another area where vulnerabilities can be introduced into a system. It is good practice to carefully review and examine this code to verify common errors, such as sign and overflow errors, do not occur. Errors which when manifested, can lead to unexpected system behavior. Specific recommendations provided by the DNP Users Group for suppliers developing products which implement DNP3 and DNP3-SA include:

- Appropriate variable types should be used to avoid integer overflows, truncation, or negative numbers. Calculations based on index ranges require the use of integer types with a larger bit-width than the size of the index contained in the message (e.g., a count of objects in a 2-byte start/stop header could use a 32-bit integer for correct representation).
- Avoid unintended sign extension by masking values when copying from smaller to larger integers. This especially applies when reading a value from a character array into an integer type. Unsigned declarations don't always work as expected.
- Ensure that sign bits and truncation are handled correctly when translating 48-bit DNP3 time to 32-bit internal timestamps.

B.6 Software Life Cycle

Poor software handling and development practices increase the opportunity of introducing hidden vulnerabilities within the end products that if exploited, can potentially result in significant impacts to a utility which has deployed them. It is recommended by the DNP Users Group that suppliers developing products which implement DNP3 and DNP3-SA adopt a holistic Security Development Life-cycle (SDLC) that includes code reviews, static & dynamic analysis, and fuzz testing.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002003736

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com