Further Information Regarding the Release of DNP3 Secure Authentication Version 5 (SAv5)

1 December, 2011

Contents

Further Information Regarding the Release of DNP3 Secure Authentication Version 5 (SAv5) 1

Introduction 2

What are SAv2 and SAv5 and where can I find them? 3

Why make these changes at all? 3

What changes are being made to Secure Authentication? 4

Why does the Users Group announcement about SAv5 say that SAv2 is “deprecated”? And what does that mean for my installation? 5

I think you are saying that I must not use SAv2. But my equipment vendors don’t have SAv5 yet. How can I implement DNP3 security? 6

How should I be implementing security? 7

What new procedure is the DNP Users Group considering for handling future security revisions? 7

Why does IEEE 1815 look different from the DNP3 Specification available on the Users Group Website? 8

Can you summarize what this was all about? 8

Introduction

On 7th November, 2011, the IEEE announced that work was proceeding to update IEEE 1815™, the standard defining the DNP3 Specification (http://standards.ieee.org/news/2011/1815dnp3.html). The revisions include a significant update to the Secure Authentication section of the specification. The IEEE balloting procedure to adopt these updates is expected to commence in January, with publication of the revised IEEE 1815 coming later in 2012. This IEEE announcement has been reported in a number of control system technical journals and websites.

In coordination with the IEEE announcement, the DNP Users Group published a more succinct announcement on 9th November stating that revisions to the Secure Authentication procedures of DNP3 have been completed and are now available (dnp.org). The new Secure Authentication Version 5 (SAv5) procedures supersede all earlier versions, including the Version 2 procedures (SAv2) that were included in IEEE 1815-2010. This announcement also indicated that SAv2 should not be deployed in new installations and that SAv2 and SAv5 procedures are not directly interoperable.

One of the primary purposes of both announcements was to advise that an updated security procedure has been developed that replaces the previous version and that it is recommended that the new version be used in new deployments.

The DNP Technical Committee is aware that there are field deployments using SAv2. These systems can continue to be used. There are no mandatory requirements to remove, replace or update existing deployments to SAv5. SAv5 is recommended for new deployments. There are unavoidable incompatibilities between SAv2 and SAv5 that do not permit a device that ONLY implements SAv5 to support authenticated communication with a device that ONLY implements SAv2. However, interoperability between SAv2 and SAv5 can be achieved if devices that support SAv5 can be configured to use SAv2 to communicate with devices that cannot support SAv5.

It has been recognized by the DNP Users Group Steering and Technical Committees that the November 9th announcement of a change to DNP3 was not done in the usual manner: Normally a proposal and a vote to approve its adoption are presented to the membership at the same time. Furthermore, it is the opinion of the Steering and Technical Committees that security revisions have special criteria that may not fit well within the current guidelines for protocol updates. In recognition of this, the Steering Committee intends to propose a new method for incorporating security revisions into DNP3. Further details of this proposal will be released in the near future and it is expected that the proposal will be voted on at the Users Group Annual Meeting in January 2012.

A special email address has been set up for comments and questions regarding these changes: secure_authentication@dnp.org. Some clarifications about these announcements have been requested. This notice seeks to provide additional information to address some of the concerns raised in those queries, formatted as a set of Questions and Answers. Readers of this notice who have further questions or comments are invited to submit them to this email address.

What are SAv2 and SAv5 and where can I find them?

DNP3 Secure Authentication 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. SAv2 and SAv5 are revisions two and five of this part of the DNP3 Specification.

All DNP3 Specification documents are available to members of the Users Group through the document library and the document historical archive on the DNP Users Group website. In association with the announcement of the release of SAv5, the new version has been made publically available so that it can be accessed by any interested party, not just by Users Group members.

The links to these documents are:

SAv2: DNP3 Vol2-Supp1 Secure Authentication v2 2008-07-31
(included in IEEE 1815-2010)

SAv5: DNP3 Secure Authentication v5 2011-11-08
(to be included in IEEE 1815-2012)

Why make these changes at all?

Cyber security is a dynamic environment. A goal of security is to enhance the ability of systems to operate correctly, even in the presence of unexpected conditions or when subject to deliberate attempts to interfere with that correct operation. There are many different techniques that enhance cyber security and various techniques can often be used in combination to provide resilience against specific sets of potential problems or vulnerabilities. DNP3 Secure Authentication provides services to authenticate the sender and the content of messages.

Over time, new security threats will be discovered and new methods devised to compromise existing techniques. Sometimes new problems appear that were previously not imagined. One way in which security problems differ from random errors is that security flaws may be actively investigated and exploited by a malicious actor. As new techniques are developed that expose or exploit security flaws, new measures need to be developed to address those changes and maintain system security. This is an on-going cycle that never ends. New versions of DNP3 Secure Authentication will be released from time to time as required to address the changes in the evolving threat landscape.

Methods that were once thought to be secure have since been “cracked”. One must consider that any security method will have a limited lifespan and will be superseded by future revisions that are needed to address flaws that are found in those methods.

What changes are being made to Secure Authentication?

There are three drivers for the changes between SAv2 and SAv5:

1. Addressing evolving security threats

   In developing SAv5, the operation of DNP3 SA has been reviewed by independent external security experts. A number of features in SAv2 and in the SAv3 and SAv4 drafts were identified as being potentially vulnerable. Additionally, the Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has a set of security criteria that must be met in order to permit IEEE 1815 to be adopted as a recommended standard for use in the Smart Grid. Some modifications that appear in SAv5 were included in order to meet SGIP security requirements.

   Some specific message exchange sequences described in SAv2 have been modified in SAv5 in order to enhance security by reducing the probability of denial-of-service attacks.

   Some option settings (in particular the use of SHA-1) that were permitted in SAv2 are now considered to be “relatively insecure”. These options are still permitted in SAv5, but the configuration requirements are changed so the selection of these settings must not be the default value of those options. Additionally, devices supporting these settings must be configurable to reject run-time requests to use these settings. The reason these settings were retained is for compatibility with severely resource-constrained devices whose performance is only sufficient to support these “entry level” options. When the choice is between “low security” and “no security”, the entry level options in SAv5 still allow the use of “low security”.

2. Correcting faults that have been found in SAv2

   Some operational incompatibilities have been found in the procedures defined in SAv2 where communication between a pair of devices is disrupted because each requires the other to provide security information before communication can proceed. These errors primarily relate to sequences used in unsolicited reporting and are corrected in SAv5.

   Unfortunately, the correction to this fault necessitated a non-interoperable change in the procedures for both polled and unsolicited reporting. Security using SAv2 and security using SAv5 have differences that could not be harmonized to allow them to directly interoperate. For this reason, the Secure Authentication implementation of SAv5 devices is not interoperable with SAv2 devices.

   However, a device that supports SAv5 could use secure authentication with a device that only supports SAv2 if the SAv5 device includes a configuration option (and appropriate software support) to use either the SAv2 or the SAv5 procedures when communicating with other devices. As future Secure Authentication revisions are released, this configuration selection will need to be extended to select the Secure Authentication version being used for communication between each pair of devices.

3. Adding remote key-management functions

   In SAv5, the DNP Technical Committee added the ability to remotely update the security keys (the "Update Key") in a remote device. This extra functionality can use either symmetric or asymmetric methods with several implementation options.

   This additional functionality is optional: SAv5 can use "Pre-shared Update Key" mechanisms (as used in SAv2) if there is no need to support remote key change. When used in this manner, there is little difference in the amount of software and processing power required to support SAv5 compared to what was required in SAv2.

There are many detail differences between SAv2 and SAv5. A summary of these differences is attached as an appendix to this announcement.

Why does the Users Group announcement about SAv5 say that SAv2 is "deprecated"? And what does that mean for my installation?

Due to the evolving nature of security requirements, it is sometimes necessary to migrate from old security techniques to new techniques. Sometimes the change only requires adding new functions or features, but sometimes it will require removal of previous functionality or options in order to prevent them from being exploited. SAv5 includes a combination of adding new features and also of changing the operation of some features that appeared in SAv2.

The release of SAv5 addresses some security weaknesses that exist in SAv2 and changes the requirements for selection of some security options. These changes were required for IEEE 1815 to be accepted in the SGIP catalog of standards. Because SAv5 is not simply an extension of SAv2 but replaces some functionality of SAv2 with incompatible requirements, they cannot coexist in the specification and SAv5 must replace SAv2. Thus SAv2 becomes deprecated and is no longer recommended for use in new installations.

It is understood that there is delay between the announcement of a change to a specification, such as this release of SAv5, and the availability of software or devices that implement those revisions. This will be the case no matter how or when the change is announced.

Systems that are currently deployed that use SAv2 or that will be deployed before SAv5 implementations become available, should continue to use SAv2 as this provides a significantly higher level of operational security than basic DNP3 without secure authentication. There will be a transitional period as devices that support SAv5 become available.

It is anticipated that early deployments of devices with SAv5 may include a configurable "SAv2 compatibility" setting that allows them to communicate with other devices using either SAv5 procedures or SAv2 procedures. Over time, support for SAv2 will become less common. In the same way, future updates to DNP3 Secure Authentication may require optional support for multiple different SA versions in one system.

It is recommended that systems using SAv2 be migrated over time to support SAv5 if this is possible.

It is expected that some SAv5 systems will only support the “pre-shared key” mode of operating that is similar to SAv2 operation and will not adopt the remote key change functionality. Full adoption of SAv5 remote key change capability involves support for additional features such as access to a Certificate Authority. Some users will choose to deploy this full remote key change functionality, some will not.

I think you are saying that I must not use SAv2. But my equipment vendors don’t have SAv5 yet. How can I implement DNP3 security?

That is not what we meant. The announcement about SAv5 deprecating SAv2 was intended to advise that the new specification includes SAv5 and no longer includes SAv2. We meant this to be understood as an announcement that there is a change coming.

Obviously, it takes time after announcement of any change for that change to appear in products. We expect that systems currently in the procurement / deployment cycle will be using SAv2 and will continue to use SAv2 until SAv5 can be adopted. End users should talk to their suppliers about updating their equipment to use SAv5. We recommend shifting to SAv5 as early as can be managed. Note that if you currently use SAv2, you are using a procedure with pre-shared security keys. It is possible to use SAv5 in this same way and doing so uses similar resources (memory, CPU cycles, etc.). From a technical standpoint, a device that can support SAv2 should be able to be reprogrammed to support SAv5.

In the near future, the DNP Users Group will be developing guidance regarding the migration timeline for security revisions. End users should account for this planned migration and have logistics in place to do this as rapidly as possible. Exploits may be released very suddenly with little or no warning. Because there is no control over the release of such exploits, it would be wise to have plans in place for operations with compromised security.

Expect to see a continuing series of security revisions. The Users Group committees will always endeavor to ensure that the compatibility between versions will be as seamless as possible; but the nature of security is such that sometimes this cannot be done. The DNP Users Group is considering changes in policies for handling security revisions so as to make this transition process both as orderly and rapid as possible.

Notwithstanding this announcement and the recommended migration from SAv2 to SAv5, we also understand that users with an existing SAv2 deployment may wish to continue using that system as is without updating it. Such a system may be progressively more difficult to maintain in the future as fewer devices will continue to offer support for SAv2, but in the short term this is a viable strategy if there is no external driver enforcing the update.

How should I be implementing security?

This notice does not seek to be a tutorial on control system cyber-security, however, readers are reminded that:

- Control system security generally requires an on-going, proactive approach. Security requirements change over time and maintenance of system security will require on-going review and evolution of policies, procedures, architectures, tools and training.
- System owners should consider putting in place procedures to permit rapid response to changes in the security landscape, whether to implement updated tools, methodologies or procedures; to respond to attacks or to ensure business continuity in the aftermath of a security breach.
- Deploying security updates should be considered “normal business”.
- Multi-layered security postures should be considered as they can provide multiple lines of defense and may offer additional safeguards under conditions where one or more security measures are rendered obsolete or require revision.

What new procedure is the DNP Users Group considering for handling future security revisions?

The DNP Steering Committee and DNP Technical Committee recognize that security is a “moving target” and anticipates that there will be a series of revisions to the Secure Authentication Mechanism issued in the future. It is anticipated that these releases will address changes in the security challenges being faced at those future dates. By the nature of how they work, security revisions may not always maintain full backwards compatibility from one version to another. Some form of transitional arrangement needs to be put in place. The proposed format for this has yet to be finalized, but it may take a form similar to the list presented below. This will be discussed and put to a vote by members at the DNP Users Group Annual Meeting in January 2012.

A possible format for enforced evolution could be:

a. At some date, a new security version is announced
b. In association with the announcement of the new version, a “target date” will be announced
c. The requirement for compatibility may be that devices implementing the new version before the target date must also provide compatibility with the current version *AND*
   All devices supporting the older version must support the newer version by the target date *AND*
   New devices shall not support the older version after the target date

An alternate possibility:

a. At some date, a new security version is announced

b. In association with the announcement of the new version, a “target date” will be announced that allows time to develop revised software and also a “changeover date” after which the previous version shall not be supported
c. New devices will be required to support the new version from the target date
d. Between the target date and changeover date, new devices should support the new and old versions (by configuration)
e. After the changeover date, new devices should not support the old version
f. During the period between the target and changeover dates, security software support in deployed devices should be updated to the new version

Depending on the reason for the security revision and the complexity of the revisions, the span of time from announcement to the target and changeover dates may vary considerably.

It will be recommended that system users update the security support in their systems so that all devices may be migrated to the new version by the changeover date, but it is recognized that users may choose to leave an existing implementation running with whatever security version it had when installed.

It is possible that, in some countries, government or industry regulatory bodies may impose rules requiring the adoption of specific security techniques or termination of the use of certain techniques by specific dates.

Why does IEEE 1815 look different from the DNP3 Specification available on the Users Group Website?

IEEE standards conform to a specific format and set of rules. During the creation of IEEE 1815, the DNP3 Specification was reformatted and edited to conform to the IEEE format.

Work is now underway to harmonize the DNP3 Specification document to the IEEE format. In the near future, the DNP3 Specification available on the Users Group website will have identical content and format to the published IEEE 1815 standard.

Can you summarize what this was all about?

Here’s a bullet list of points:

1. SAv2 was developed to address requests from the user community to provide a mechanism to authenticate DNP3 traffic. SAv2 provided support for pre-shared symmetric keys only.
2. SAv5 was developed to address requests from the user community to provide a mechanism for remote key change as an extension to the capabilities provided in SAv2. SAv5 provides support for pre-shared symmetric keys and also for remotely changing keys by symmetric or asymmetric (Public Key Infrastructure) methods.
3. In addition to the remote key change mechanisms, SAv5 corrects a problem identified in operation of unsolicited communication using SAv2 and also improves the security resilience offered by SAv2 under specific attack scenarios. Some features and recommendations

provided in SAv5 address specific cyber-security vulnerabilities identified after review by independent cyber-security experts.

4. It is possible to implement a subset of SAv5 at the same level of functionality as SAv2 by only implementing the pre-shared symmetric key mechanisms. When this is done, the complexity of implementation is approximately equivalent to the complexity of implementing SAv2.
5. Despite concerted effort, some details of the operation of SAv2 and SAv5 cannot be harmonized and backwards-compatibility is not possible. Consequently, a device that only supports SAv2 cannot operate securely with a device that only supports SAv5. However, it is possible to support both and select which one will be used for each station. In practice, this will usually mean that a master device will be configurable to support SAv2 or SAv5 procedures when communicating with a particular outstation that supports only one version or the other. If both devices support both versions, SAv5 procedures should be used, even if the system uses pre-shared keys and does not operate in remote key exchange mode.
6. Both the IEEE and the DNP Steering Committee believed it was important to advise the user community as early as possible about this change from SAv2 to SAv5 so as to minimize the impact that will occur if larger numbers of SAv2 devices and systems are deployed before advice is issued about the change to SAv5
7. The normal procedure for adoption of modifications to the DNP3 Specification that affect backwards compatibility is to present these changes to the Users Group membership for approval. This has not occurred for this particular change to adopt SAv5 in place of SAv2. In part this is due to the separate review and approval processes used by the DNP Technical Committee and the IEEE, who are striving to work together to merge all existing differences into a single common specification.
8. The user community will have the opportunity to formally accept (or reject) SAv5 in the IEEE balloting process and also within the DNP Users Group by vote at the Annual Meeting. We understand that the wording of the announcement made it appear that the UG membership was not being given the opportunity to approve the adoption of SAv5. This was due to a lack of clear focus on procedure and we apologize for this error.
9. A new policy for handling the announcement of future security revisions is being formulated by the DNP Steering Committee and DNP Technical Committee for consideration by the Users Group membership. Details of this new policy proposal will be released shortly. The Users Group will be asked to vote on the adoption of this new policy at the DNP Users Group Annual Meeting in January, 2012.

Appendix: Changes between DNP3 Secure Authentication Version 2 and Version 5

The changes to the Secure Authentication specification fall into the categories described in Table 1.

Table 1 – Categories of Changes between Version 2 and Version 5

Category of Change	**Description**	**Purpose**	**Compatibility Issues**
Remote Update Key Change	In Version 2, Update Keys were pre-configured at the master and outstation. Version 5 adds objects and procedures for remotely changing Update Keys, which may involve transmitting standardized X.509 certificates.	Reduce costs by eliminating the need to send personnel to remote sites.	None. Version 5 specifies that the Update Key changing methods are optional, and pre-configuring Update Keys is still permitted.
Security Statistics	Version 5 adds objects and procedures for maintaining and reporting statistics about the operation of the Secure Authentication protocol, e.g. the number of authentication failures.	Help users to identify patterns of behavior that may indicate attacks.	A Version 2 master 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.
Throttle Sending Error Messages	Version 5 specifies fewer cases than Version 2 in which the device sends an Error message. Version 5 devices now only send Error messages for configuration errors, not operational errors like timeouts or unexpected messages. In these cases the device simply discards the incoming message silently.	Reduce the impact of some types of denial-of-service attacks.	None. In most cases, the Version 2 device is not expecting a reply. In other cases, the Version 2 device will wait for a Reply and then experience a Reply Timeout. The timeout will cause it to take the appropriate recovery action, just not as quickly.
Critical Confirms	Version 2 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. Version 5 clarifies a few specific situations that the devices must handle in order to make this possible.	Permit devices to authenticate Application Confirms	The case in which the Challenge was itself contained in an Aggressive Mode Request was not previously specified. Version 2 implementations that did not consider this possibility may not send the Confirm in Aggressive Mode as requested.
Throttle Changing Session Keys	Version 2 masters change Session Keys after a configured number of authentication errors. Version 5 masters will only change Session Keys for this reason a configured maximum number of times, and then revert to changing Session Keys at the configured change interval.	Reduce the impact of denial-of-service attacks from devices always sending bad authentication information	None. A Version 5 master will change Session Keys less often if faced with multiple authentication errors, but it will always change them at least as often as the Version 2 outstation is configured to expect.
Unsolicited Responses	Version 2 did not adequately address all the possible interactions between solicited and unsolicited Secure Authentication messages passing each other in transit. To address these interactions, Version 5 changes the calculation of Challenge Sequence Numbers (CSQ) and specifies that separate Challenge Data must be used for solicited and unsolicited communications.	Permit secured unsolicited responses to be transmitted in addition to secured requests and solicited responses.	This is the primary incompatibility between Version 2 and Version 5. The two versions will not calculate the correct expected CSQ in some cases, causing incorrect authentication failures.

Category of Change	**Description**	**Purpose**	**Compatibility Issues**
Restarts	Version 2 did not adequately specify exactly what should happen when an outstation or master restarts, particularly regarding the initialization of Session Keys. Version 5 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. Version 5 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.	Ensure that the restart of an outstation does not cause an excessive number of authentication failures and a long delay before data can be exchanged.	A Version 2 master might challenge an initial Null UR instead of immediately changing Session Keys, causing multiple authentication failures but eventually causing a reset of the Session Keys. A Version 2 device might try to send an Aggressive Mode Request immediately after a Session Key change instead of waiting for a Challenge/Reply to take place.
Continues Waiting	Version 2 specifies that if a device receives an unexpected message while waiting for a particular Reply, in most cases it should stop waiting for the Reply and act on the new message, in order to re-establish normal communications as soon as possible. Version 5 assumes that such unexpected messages could be attacks and specifies instead that the device should discard the unexpected message and continue waiting for the Reply as before.	Reduce the impact of denial-of-service attacks from unexpected messages.	None. If there is no attack underway, the device receiving the unexpected message will time out waiting for the Reply and will Challenge the next critical message, re-establishing normal communications. This will take longer to recover than the Version 2 solution in the case of an error but does not permit unmitigated control of the device in the case of an attack.
New Algorithms	Version 5 adds cryptographic algorithms not supported by Version 2 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.	Provide better security than specified in Version 2 and allow for advances in the capabilities of attackers.	All the Version 2 algorithms are still permitted in Version 5, with one exception: A Version 5 device is not required to support the mandatory Version 2 TLS cipher suite. Implementations that wish to communicate with both Version 5 and Version 2 devices must support a superset of the cipher suites. In addition SHA-1 is no longer the default MAC algorithm so any Version 5 device must be explicitly configured to use it Note: The Version 5 specification now uses the generic term MAC instead of HMAC since HMAC is a specific type of MAC.
Key Status HMACs	Version 2 specifies that the HMAC on a Key Status message need not be supplied unless the Key Status is OK. Version 5 specifies that if the outstation has a previously valid Session Key, it should include the HMAC using this old key even if the current Key Status is not OK.	Provide better assurance that an attacker is not attempting to cause a denial-of-service attack by sending bad Key Status messages.	None. Version 2 device will likely ignore the HMAC if the status is not OK. If it does not ignore the HMAC, it will likely consider the Key Status message invalid, in which case it will eventually reset the Session Keys, which is what is desired in any case.

Category of Change	Description	Purpose	Compatibility Issues
Other	There are several other changes added to Version 5 that do not fall into any of the other categories:		
	• Added rule that a master should either wait for challenges to NO ACK function codes, or send them in aggressive mode.	Avoid requests colliding with challenges if the master doesn't wait.	None. Version 2 devices should permit sending any particular requests in aggressive mode.
	• Added rule that master is not required to challenge responses to requests that cause a restart. Noted outstations may restart without waiting for a challenge.	Avoid delays waiting for authentications that are needless since device is restarting.	None. Version 2 outstations may do this anyway and there's nothing the master can do about it.
	• Changed configuration and file operations to mandatory critical operations.	Prevent attackers from reconfiguring outstations to not require authentication.	None. Version 2 specifies that a device may decide that any operation is critical, so compliant Version 2 devices will be able to respond appropriately.
	• Added rule that the receiver shall set their CSQ to that found in an aggressive mode request UNLESS it is already larger than that found in the request.	Allow some flexibility due to the changes made to the CSQ calculation.	None. Actually helps with compatibility.
	• Cancels the Reply Timer when an Invalid Reply is received, even if no Error message was sent	Adds an action that is logical but was not specified.	None. Internal and does not affect the communications traffic. Version 2 devices likely do this anyway because it's logical.
	• Outstation only sets Key Status to COMM_FAIL rather than NOT_INIT or AUTH_FAIL when Max Reply Timeouts is exceeded.	Clarifies an ambiguous situation.	None. Key Status values are documentation only. The Version 2 master should not be looking for a particular Key Status value other than OK or not OK.
	• Outstation only responds to Key Status Request if the USR is valid, otherwise discards it.	Adds an action that is logical but was not specified.	None. Version 2 devices likely do this anyway because it's logical. If not, the status must be not OK and the master will respond appropriately.
	• Sends an Error message if Aggressive Mode is disabled and an invalid request is received.	Adds an action that was logical but was not specified.	None. Version 2 devices likely do this anyway because it's logical. If not, ignoring the Aggressive Mode Request is a valid response.
	• Master resets session keys if it has just restarted and receives Key Status OK	Adds an action that was logical but was not specified.	None. If the Version 2 master tries to send a critical request without first resetting the keys, it will be challenged by the outstation and the authentication will fail, eventually causing the master to reset the session keys anyway.
	• Added rule that master can optionally decrease the Session Key change interval exactly once due to authentication failures	Permits a master to adjust to the most likely reason for an authentication failure: misconfiguration of the timers.	None. Version 2 outstation will accept a key change whenever it occurs.
	• Added rule that the Key Change Interval Count can be no more than half the maximum Key Change Sequence Number	Avoids vulnerability due to counter roll-over concerns.	None. The receiver of the KSQ does not check it other than to verify it is the correct one for the current key change.

Category of Change	Description	Purpose	Compatibility Issues
	• Added rule that if the maximum number of authentication failures is exceeded, the device shall drop the TCP connection.	Reduce the impact of denial-of-service attacks.	None. Version 2 devices will re-establish the TCP connection if needed.