7 SECURE AUTHENTICATION

7.1 Purpose

The purpose of this standard is to define a protocol mechanism that:

- A DNP3 outstation can use to unambiguously determine it is communicating with a user who is authorized to access the services of the outstation.
- A DNP3 master can use to unambiguously determine that it is communicating with the correct outstation.

This specification is fundamentally based on IEC 62351-5.

7.2 Threats Addressed

This standard shall address only the following security threats, as defined in IEC 62351-2:

- Spoofing
- Modification
- Replay
- Eavesdropping - on exchanges of cryptographic keys only, not on other data.

7.3 General Principles

This subclause describes the guiding principles behind this standard, based on the identified threats.

7.3.1 Authentication Only

This standard addresses authentication only, not encryption or other security measures. It does not rule out the possibility of such measures being added to DNP3 later or through the use of external measures such as “bump in the wire” link encryptors.

7.3.2 Application Layer Only

This standard describes authentication at the application layer. Application layer authentication is necessary because:

- DNP3 must be used over a variety of different physical networks and may be “bridged” from one to the other, as in the case of a TCP/IP terminal server or IP radio. Only authentication at the application layer will ensure end-to-end security.
- Application layer authentication permits the possibility of protection against “rogue applications” that may be co-resident with the DNP3 application and attempt to use the DNP3 link without authorization.
- Application layer authentication permits the possibility of authenticating individual users, as discussed in 7.3.9.

7.3.3 Bi-directional

This standard describes a mechanism that can be used in either transmission direction, master-to-outstation (controlling direction) or outstation-to-master (monitoring direction).

7.3.4 Challenge-Response

The mechanism described in this standard is based on the common security concept of challenge and response. This principle has been applied for the following reasons:

- It places the responsibility for security on the device that requires authentication, which is more practical in a diverse network such as those found in the utility industry.
- It permits some communication to be left unsecured if desired, reducing bandwidth and processing requirements.
- It works effectively in a non-connection-oriented environment.

Because “response” is a keyword in DNP3, the term used in this standard is “reply”.

7.3.5 Pre-Shared Keys

This standard permits pre-shared keys to be used by default. This principle recognizes the fact that many utilities may choose not to manage security credentials in a more sophisticated manner but nevertheless require some level of protection.

This standard also provides optional methods to remotely change pre-shared keys using either symmetric or asymmetric (public key) cryptography.

7.3.6 Backwards Tolerance

This standard recommends that the following conditions be satisfied when a secure device (one implementing this authentication mechanism) communicates with a non-secure device:

- The secure device must be able to detect that the non-secure device does not support the authentication mechanism.
- The non-secure device must continue to operate normally after being contacted by the secure device. In other words, the authentication message cannot cause the non-secure device to fail.
- The two devices must be able to continue to exchange information that is not considered critical.

However, the mechanism’s ability to meet these conditions is largely dependent on the quality of the implementation on any particular device. This standard therefore recommends that secure devices avoid sending security messages if it is not known whether the remote device supports security.

7.3.7 Upgradeable

This standard permits system administrators to change algorithms, key lengths, and other security parameters to deal with future requirements. In keeping with the principle of backward tolerance, it also permits one end of a link to be upgraded at a time.

7.3.8 Perfect Forward Secrecy

This standard follows the security principle of perfect forward secrecy, as defined in IEC 62351-2. If a session key is compromised, this mechanism only puts data from that particular session at risk, and does not permit an attacker to authenticate data in future sessions.

7.3.9 **Multiple Users and Auditing**

This standard assumes that there may be multiple users of the system located at the site of the master. It provides a method to authenticate each of the users separately from each other and from the master itself.

The intent of this principle is to permit the outstation to conclusively identify the individual user (not just the device) that transmits any protocol message. This information can be used to create an audit trail, which NIST defines as "A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period". The creation of such an audit trail is out of the scope of this standard, but some recommendations are given in 7.4.1

This standard permits outstations to limit access to certain functions, either based on the individual identities of users, or based on the "roles" the users perform. This role-based access control is only possible if one of the optional methods for remotely changing pre-shared keys is implemented.

7.4 **Theory of Operation**

This subclause describes the operation of the authentication mechanism in general terms for the benefit of first-time readers. In the case of disagreements between this overview subclause and 7.5, 7.5 shall be taken as correct.

7.4.1 **Narrative Description**

This subclause describes the operation of the authentication mechanism as a text narrative.

The assumed implementation architecture of this mechanism is shown in Figure 7-1. Multiple users may either send unauthenticated DNP messages, or may choose to authenticate selected messages. The authentication messages have the ability to distinguish between users, while normal DNP messages do not. The authentication messages are formatted as additional DNP function codes and object variations.

The software architecture used to parse, process, and distinguish between normal messages and security messages is beyond the scope of this document.

Implementers should note that logging and auditing of security events such as authentication failures is a critical part of information security. It is recommended that all implementations at a minimum log all successful and unsuccessful authentications and key changes, including the time, the DNP addresses, and the affected user. For the best forensic results, DNP devices should log entire messages, including all authentication information, so an auditor can evaluate the authenticity of the messages. However, since logging is not a part of the protocol itself, the events logged and the format of the log are not parts of this standard.

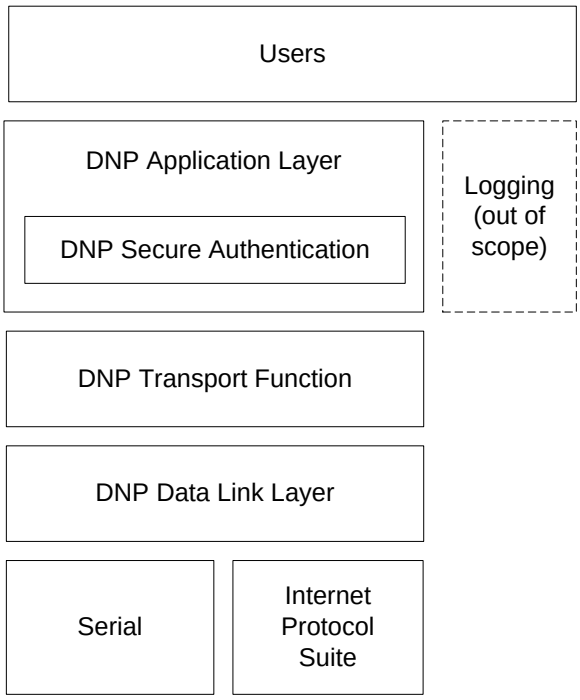


Figure 7-1: Assumed Implementation Architecture

7.4.1.1 Basic Concepts

The authentication mechanism is based on two concepts:

- A challenge and response protocol, as discussed in 7.3.4. The general mechanism is illustrated in Figure 7-3. Because "response" is a keyword in DNP3, the term used here is "reply".
- The concept of a Message Authentication Code (MAC) that both the outstations and masters calculate based on each Application Service Data Unit (ASDU, or protocol message) that is to be authenticated.

A MAC algorithm is a mathematical calculation that takes a protocol message as input, produces a smaller piece of data as output, and has the following characteristics:

- The value of the output is sensitive to small changes in the input message, so the output of the MAC can be used to detect if the message was modified.
- The calculation makes intrinsic use of a secret key that is shared by both ends of the communication.
- It is extremely difficult to determine the secret key by viewing the MAC output.
- It is nearly impossible to determine the original message from the MAC.
- It is difficult to find two messages that produce the same MAC.

There are several different types of MAC algorithms. In this version of the specification, the term MAC may refer to different variations of either the SHA-HMAC algorithm or the AES-GMAC algorithm.

This challenge-response mechanism using a MAC is a "unilateral, two-pass authentication" mechanism as described in ISO/IEC 9798-4.

7.4.1.2 Initiating the Challenge

The challenge may be initiated either by the master or the outstation.

Devices shall issue challenges to protect specific ASDUs that the device considers to be critical. The challenger issues the challenge immediately after receiving the critical ASDU, before taking any action on it.

Outstations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical. Other mandatory critical operations are described in 7.5.2.3.2. Each implementation may define additional mandatory critical operations.

To protect against replay attacks, the challenge message contains data that changes randomly each time a challenge is issued.

The challenger specifies in the challenge message the Message Authentication Code (MAC) algorithm for the responder to use when building the response.

7.4.1.3 Replying to the Challenge

The device (either master or outstation) that receives the challenge must reply before communications can continue.

The responder performs the MAC algorithm specified in the challenge message to produce the reply. A shared Session Key known to both devices is an integral part of the computation. The following types of information are included in the computation:

- A number specifying the user on the Master side is included.
- The challenge data is included, to protect against replay attacks.
- If the challenger is protecting a specific critical ASDU, data from that ASDU is also included in the computation. This protects against modification of the ASDU by an attacker.

The reply includes the resulting MAC value.

7.4.1.4 Authenticating

Upon receiving the reply, the challenger performs the same calculation on the same data used by the responder. If the results match, the challenger permits communications to continue. If the challenger was protecting a particular ASDU, it processes the ASDU.

7.4.1.5 Authentication failure

If the authentication fails, the challenger shall not use data from the challenged message. If the challenger is an outstation, it shall not perform the operation requested by the master. The challenger may then choose to transmit an error message. To help protect against denial-of-service attacks and attackers learning from repeated challenges, the challenger shall cease to transmit error messages after a configurable number of failures. Refer to 7.6.1.4.2 for more details about the configurable maximum error count.

7.4.1.6 Aggressive mode

To reduce bandwidth usage, a responder attempting a critical operation may optionally “anticipate” the challenge and send the MAC Value in the same ASDU being protected. This practice is known as “aggressive mode”. It eliminates the challenge and reply messages. For this reason, aggressive mode is optional in IEC 62351-5. However, the value of aggressive mode is considered high enough for DNP3 that all DNP3 implementations of this authentication mechanism are required to support it. Per IEC 62351-5, however, all DNP3 implementations are also required to permit it to be disabled by configuration, so that individual projects can use only challenge and reply if they choose.

Aggressive mode is a "unilateral, one-pass authentication" mechanism as described in ISO/IEC 9798-4. However, it is somewhat more secure against replay attacks than the mechanism described there, because the Aggressive Mode Request includes information from the most recently received challenge in addition to the sequence number required by ISO/IEC 9798-4.

7.4.1.7 Changing keys

Table 7-1 and Table 7-2 summarize how cryptographic keys are used and updated in this authentication mechanism. At a minimum, keys are managed by the master and by the outstation. Optionally, a trusted third party known as an *authority* may also help to manage the keys.

Table 7-1: Summary of Symmetric Keys Used

Type	Use	Change Mechanism	Range of Expected Change Interval
Monitoring Direction Session Key	Used to authenticate data transmitted in the monitoring direction by the outstation	The master encrypts the Session Key in a Key Change message using the Update Key	Minutes up to weeks (for infrequently communicating systems)
Control Direction Session Key	Used to authenticate data transmitted in the control direction by the master	The master encrypts the Session Key in a Key Change message using the Update Key	Minutes up to weeks
Update Key	The master shall use the Update Key to periodically change the Session Keys	The Update Key may be pre-shared between two devices, or if it is considered to be compromised, it may be changed remotely using either symmetric or asymmetric cryptography	Months or Years
Authority Certification Key (optional)	The authority shall use the Authority Certification Key to change Update Keys. The master shall forward the Update Key encrypted by the authority to the outstation.	The Authority Certification Key is pre-shared by the authority and the outstation and can be changed only by means external to the protocol	Years, if ever

Instead of using the Authority Certification Key, the authority, master and outstation may optionally use asymmetric cryptography, also called public key cryptography, to remotely change Update Keys. A brief summary of asymmetric cryptography follows.

Asymmetric cryptography is based around the idea that each user or device has two keys, one public and one private. The two keys are generated together and linked mathematically such that the public key may be safely transmitted in the clear as long as the private key is kept secret. An attacker cannot deduce the private key from knowing the public key. This permits the following operations:

- An entity may **digitally sign** a message using its private key. Anyone holding the public key may then verify that the message was sent by that entity and was not tampered with in transit.
- An entity may **encrypt** a message using someone else's public key. Only the entity holding the private key will be able to successfully decrypt the message.

— A trusted authority may **certify** the public key of another entity by digitally signing it. The authority usually also specifies a time period after which the public key is no longer considered valid.

Table 7-2 summarizes how these concepts may optionally be used to change Update Keys remotely.

Table 7-2: Summary of Asymmetric Keys Used (optional)

Type	Use	Change Mechanism	Range of Expected Change Interval
Authority Private Key	The authority shall use its Private Key to certify the User Public Key of a user.	The Authority Private Key is kept secret by the authority and may only be changed by means external to the protocol.	Years, if ever
Authority Public Key	The outstation shall use the authority's Public Key to validate the Public Key of a User.	The Authority Public Key may be transmitted anywhere in the clear, but must be securely installed in the outstation by trusted personnel.	Years, if ever
User Private Key	The master shall use the user's Private Key to digitally sign a new Update Key.	The User Private Key shall be generated by the user and ideally should be carried to the master in a physical token by the user. In any case, the mechanism by which the master station accesses the user's private key must be secure.	Months or years
User Public Key	The outstation shall use the user's Public key to validate the Update Key of a user.	The User Public Key shall be generated by the user and may be transmitted anywhere in the clear, but the process by which the authority certifies it must be secure.	Months or years. Even if it is not changed, it shall expire periodically and its certification by the authority must be renewed.
Outstation Private Key	The outstation shall use its Private Key to decrypt a new Update Key.	The Outstation Private Key shall be generated by the outstation and stored securely on the outstation.	Years if ever
Outstation Public Key	The master shall use the outstation's Public Key to encrypt a new Update Key for a user.	The Outstation Public Key shall be generated by the outstation and may be transmitted anywhere in the clear, although it must be installed and stored securely in the master by trusted personnel.	Years if ever

7.4.1.7.1 Managing Session Keys

The Session Keys that each device uses to hash the challenge data are the most frequently used keys. A different Session Key is used in each direction, so that if the key for one direction is compromised, it does not compromise communications in the other direction. There is a different set of Session Keys and a different Update Key for each user at the master end, identified by a User Number.

The master initializes the Session Keys immediately after communications is established and regularly changes the Session Keys thereafter. This practice of periodically changing the Session Keys protects them from being compromised through analysis of the communications link.

The master uses a second key, called the Update Key, to encrypt the new Session Keys, together with the challenge data, inside a Key Change message. The use of a second key permits the master to change the Session Key even if the original Session Key was compromised. Both the Session Keys and the Update Key are symmetric keys.

The sequence for changing the Session Keys is shown in Figure 7-7 and Figure 7-8. Like the normal authentication mechanism, it is also based on challenge and reply:

- The master sends a Key Status Request message, which contains no data but serves to initiate the process. It does include a User Number which indicates the particular Update Key and set of Session Keys being queried.
- The outstation replies with a Key Status message containing the current status of the keys and some challenge data.
- The master updates the Session Keys with a Key Change message. Besides changing the keys, the Key Change message also constitutes a reply to the challenge and permits the outstation to authenticate that the correct entity is attempting to change the Session keys.
- The outstation replies with a new Key Status message. This Key Status message indicates whether the Key Change was successful (i.e. properly received and authentic) and includes freshly generated challenge data.
- Thereafter, the master can send another Key Change message at any time, replying to the most recent challenge data it received.

The algorithm used to encrypt both the Session Keys together with the challenge data is known as a "key wrap" algorithm. The minimum required key wrap algorithms are specified in 7.6.1.2.

If either device determines that the communications between them has failed, it shall assume the most recent set of Session Keys have been compromised and shall refuse to use them to authenticate any further Challenge or Aggressive Mode Request messages. The master shall send a Key Status Request at the earliest opportunity after detecting the communications failure, and re-initialize the Session Keys.

7.4.1.7.2 Managing Update Keys

As discussed in 7.3.9, this authentication mechanism permits multiple users of the system to be authenticated separately from the master itself. Each user is identified by his or her own User Number and has his or her own Update Key and set of Session Keys. Each user may be assigned a Role designating specific actions that the user is permitted to perform.

Each user's Update Key is rarely changed. The reason for such a change is dependent on the security policy of the organization, but may include the Update Key being compromised, or a user leaving the organization.

It is vital for security that each device keeps Update Keys secret. The mechanism used to do so is out of the scope of this standard, but implementers should note that if Update Keys are entered or stored on the device in an insecure fashion, the entire authentication mechanism is compromised. It is the responsibility of each master to ensure that users are personally authenticated and securely associated with the Update Keys used to identify them.

By default, Update Keys are pre-shared by the master and outstation and must be changed by a mechanism external to the protocol. Such a mechanism must ensure that the Update Key is kept secret and cannot be obtained by eavesdropping in transit.

As already discussed, Update Keys may optionally be changed remotely using DNP3 and methods either based on symmetric cryptography or asymmetric (public key) cryptography. An overview showing the difference between the two methods is illustrated in Figure 7-2. Devices may support the symmetric method for remotely changing Update Keys, both symmetric and asymmetric methods, or neither method.

Either method requires the participation of a trusted third party known as an *authority*. The authority is necessary to certify that users are to be added or removed, or that their roles should be changed. It separates the functions of secure communications from the functions of managing Update Keys and users. No particular user of a master or outstation shall be trusted with the capability to add or remove users from an outstation, or to change the actions a user is permitted to perform. That function must be performed by a central authority whose scope is the entire organization. The authority may or may not be what is commonly known as a Certificate Authority, although it performs a similar function.

As shown in Figure 7-2, the master's job is merely to forward certifications of users to the outstation from the authority, and to ensure that the new Update Key is securely transmitted. The communications between the master and the authority for the purpose of certifying a user is out of the scope of this document but must also be secure.

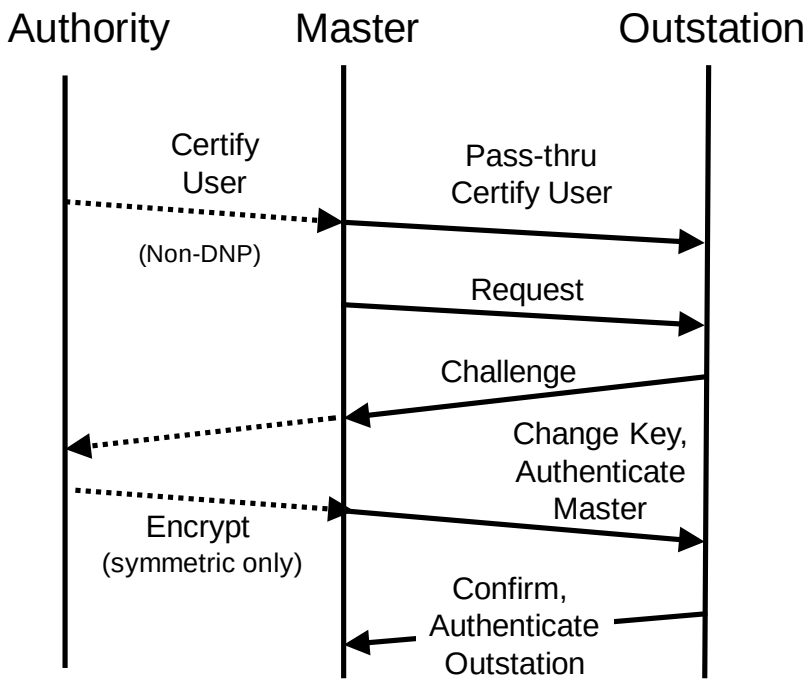


Figure 7-2: Overview of Interaction between Authority, Master and Outstation

7.4.1.8 Security Statistics

An important feature of the secure authentication mechanism is that it provides ability for the operators of the DNP network to detect some kinds of attacks. Any outstation implementing secure authentication must keep statistics on the operation of the protocol state machines and report those statistics using objects similar to normal DNP counter objects. If some statistics, e.g. authentication failures, begin to frequently exceed event reporting thresholds, it may indicate that an attack is underway. Outstations may report security statistics objects to masters *other than those involved in the authentication*. This permits the operators of the DNP network to detect attacks that may be occurring on other DNP associations than the one they are monitoring.

7.4.2 Example Message Sequences

7.4.2.1 Overview

This subclause contains diagrams illustrating examples of how the authentication mechanism shall behave and provides an overview of the mechanism. In the case of disagreements between this overview subclause and 7.5, 7.5

(which provides a formal description of the mechanism) shall be taken as correct. Bold arrows in these diagrams represent authentication-specific messages.

7.4.2.2 Challenge of a Critical ASDU

Figure 7-3 and Figure 7-4 illustrate the challenge and reply to a Critical ASDU.

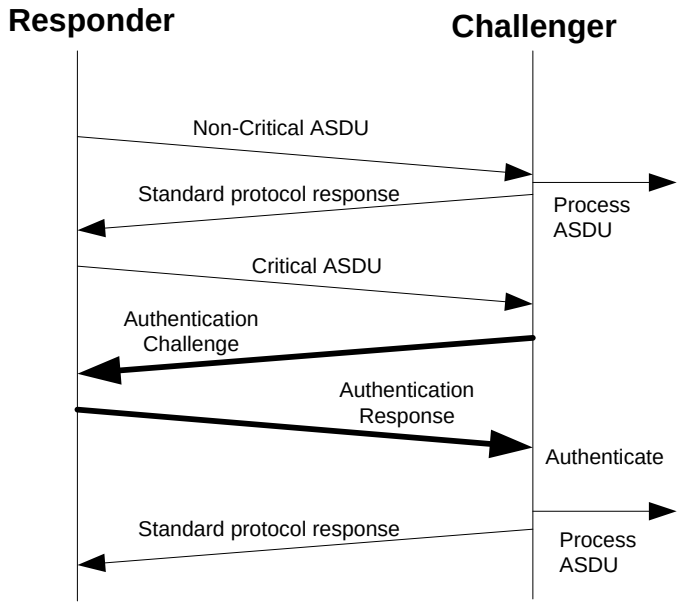


Figure 7-3: Example of Successful Challenge of Critical ASDU

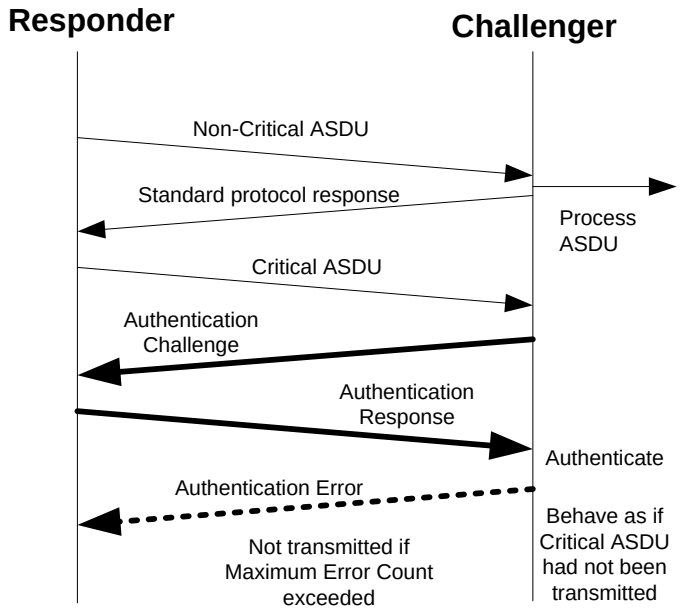


Figure 7-4: Example of Failed Challenge of Critical ASDU

7.4.3 **Aggressive Mode**

Figure 7-5 and Figure 7-6 illustrate authentication of a Critical ASDU using Aggressive Mode.

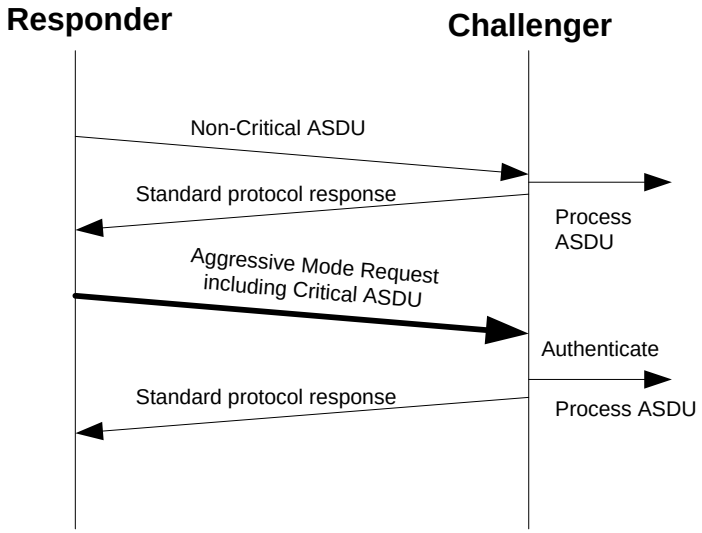


Figure 7-5: Example of a Successful Aggressive Mode Request

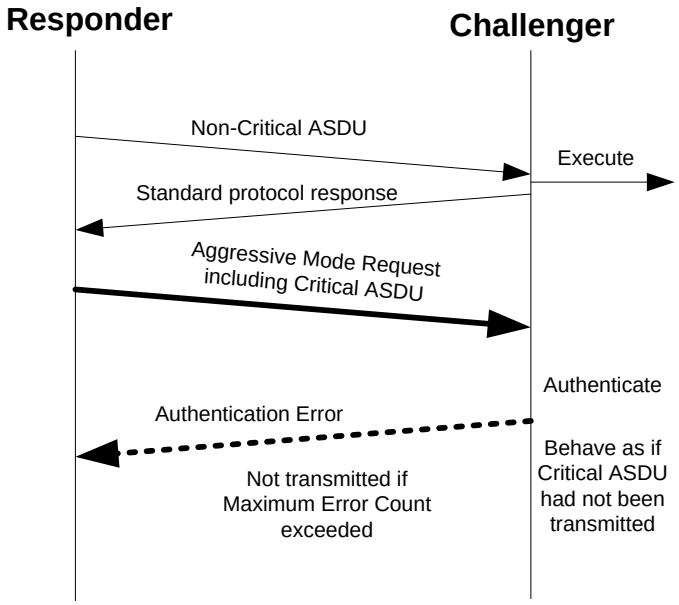


Figure **7-6: Example of a Failed Aggressive Mode Request**

7.4.4 **Initializing and Changing Keys**

Figure 7-7 and Figure 7-8 illustrate how the master initializes and changes the Session Keys on startup, periodically, and after a communications failure. Figure 7-9 illustrates how the authority and master may change the role of a user

(e.g. add a new user or give the user different access permissions) and initialize or change the Update Key for that user.

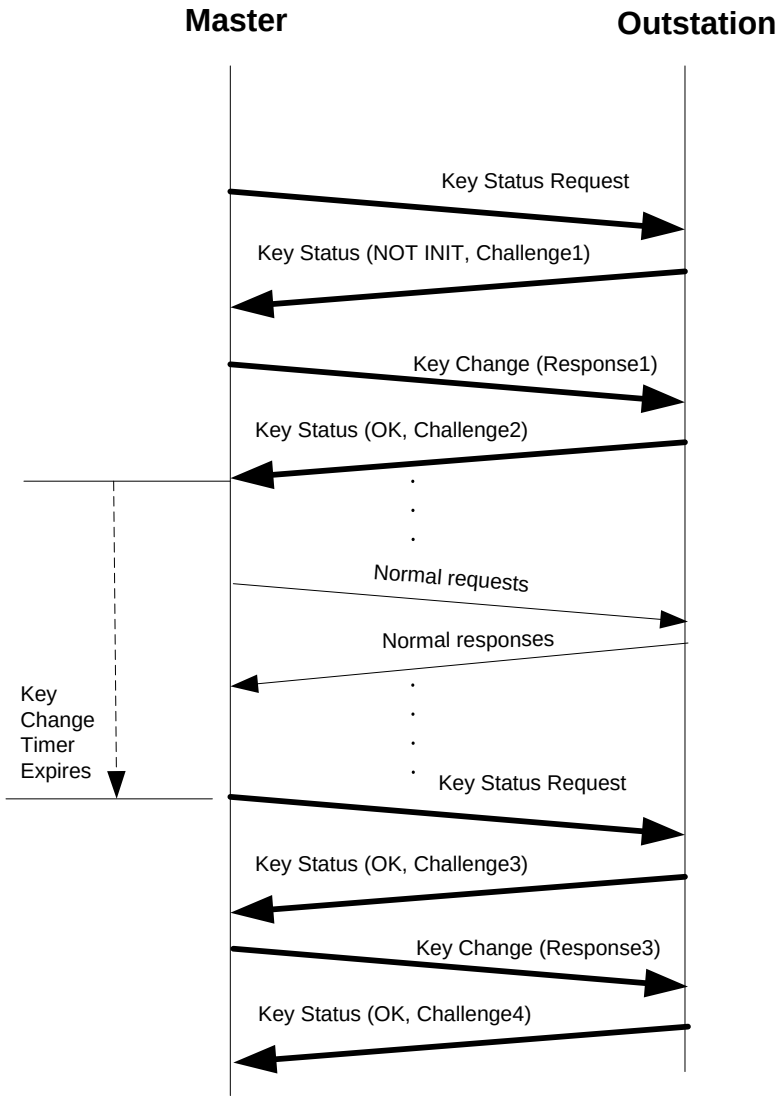


Figure 7-7: Example of Session Key Initialization and Periodic Update

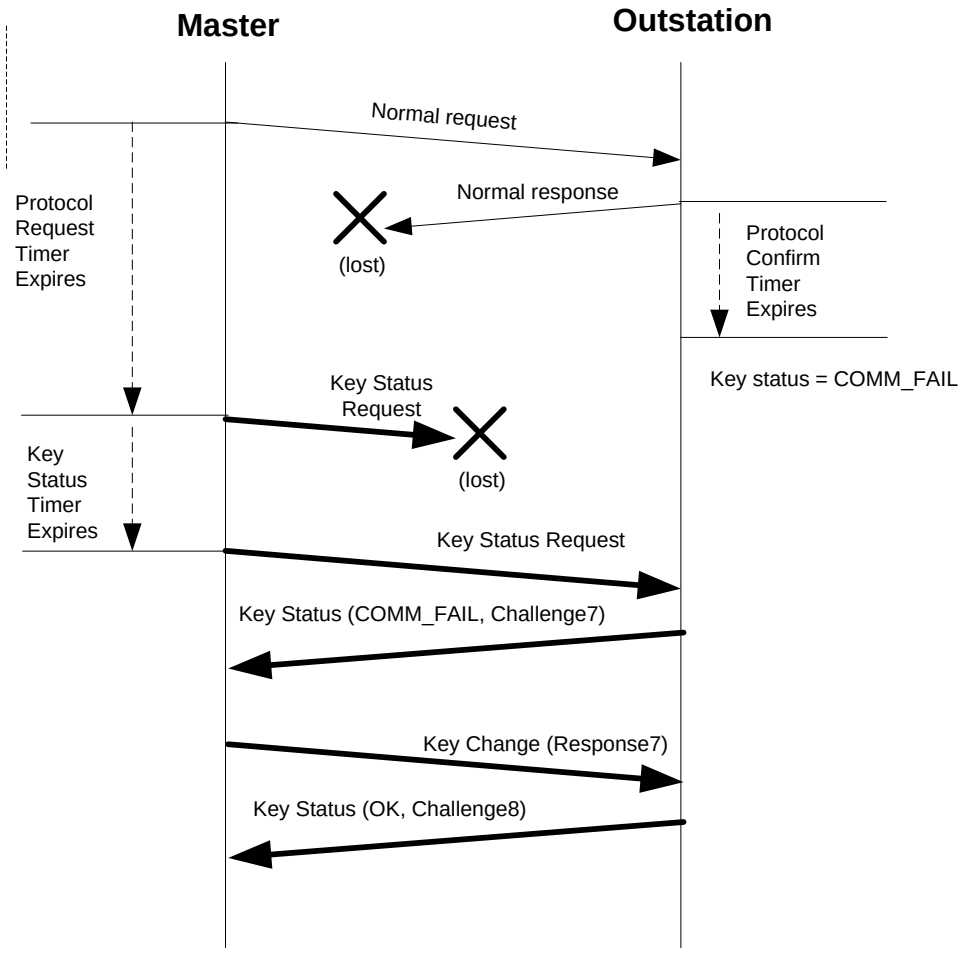


Figure 7-8 - Example of Communications Failure Followed by Session Key Change

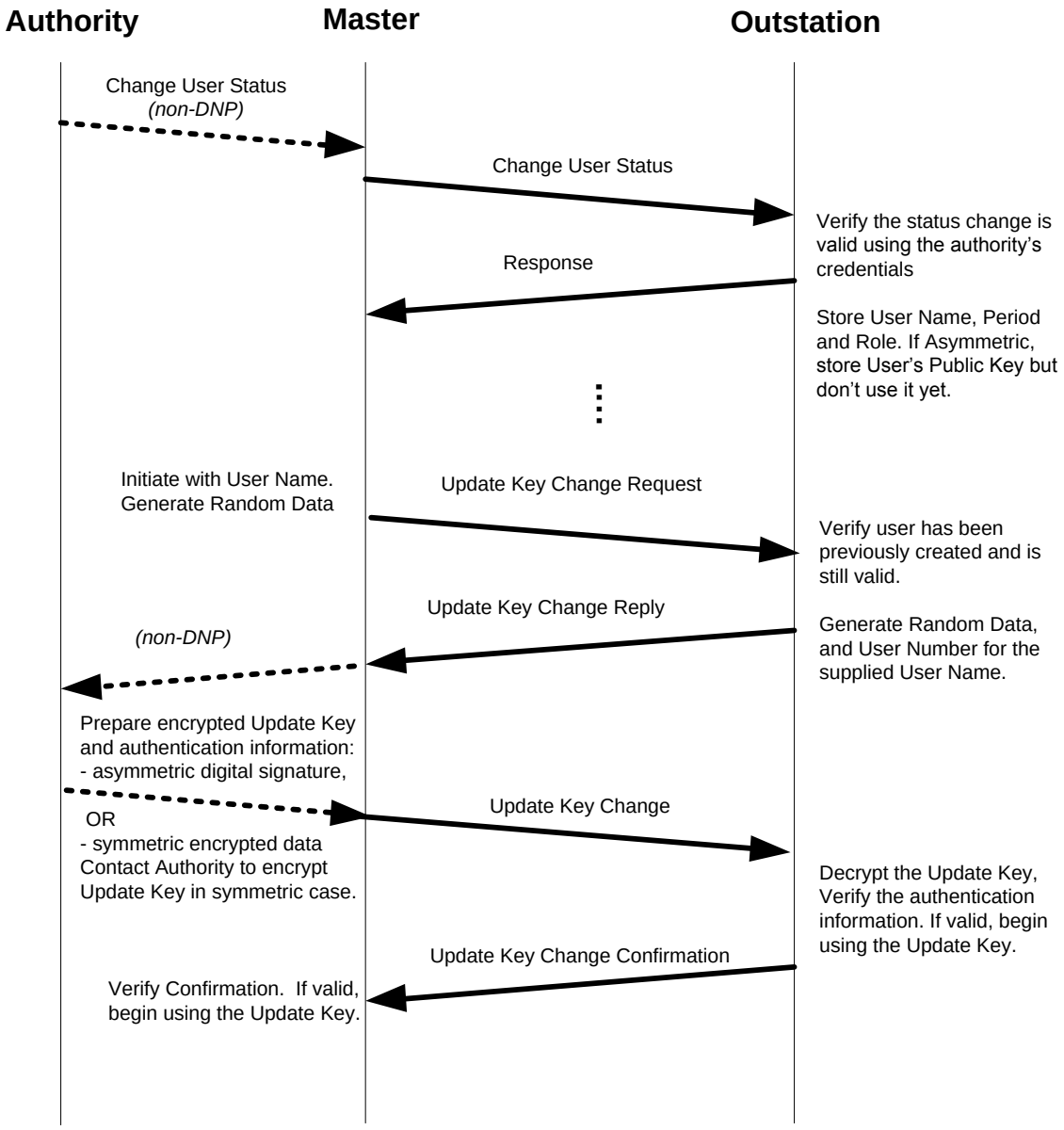


Figure 7-9 –Example of Successful User Status Change and Update Key Change

7.4.5 State Machine Overview

Figure 7-10 and Figure 7-11 show the major state transitions for the protocol, excluding the changing of Update Keys. These diagrams are not normative, nor are they comprehensive. However, these figures *are* intended to show the general operation of the authentication protocol.

The details of the state machines are specified in 7.5. If these diagrams differ from 7.5, that section shall be considered to be correct. Subclause 7.5 also contains similar figures for the state machine used to remotely change Update Keys.

The *Security Idle* and *Wait for Reply* states are common to both masters and outstations. The other states are specific to each type of device.

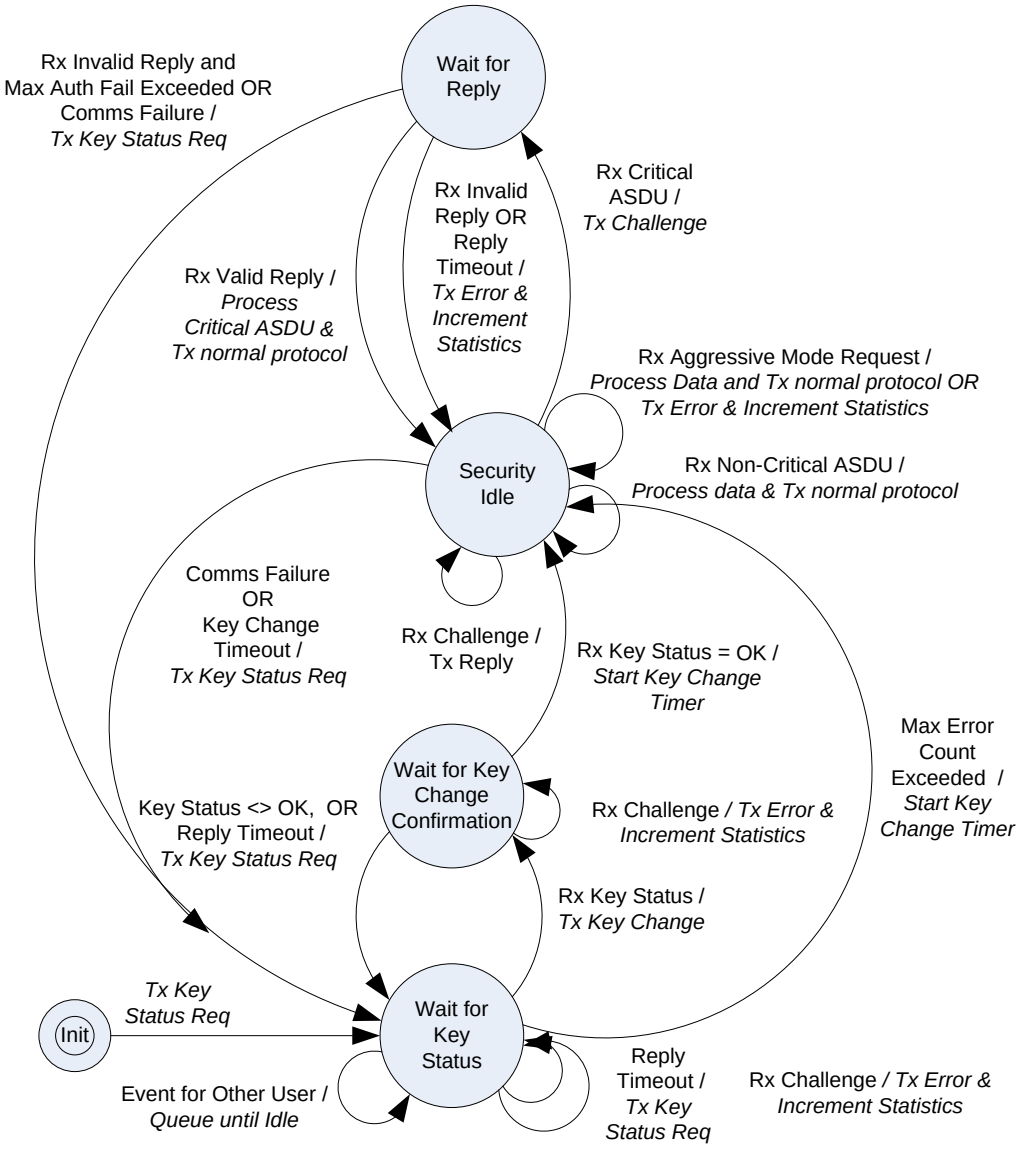


Figure 7-10: Major State Transitions for Master

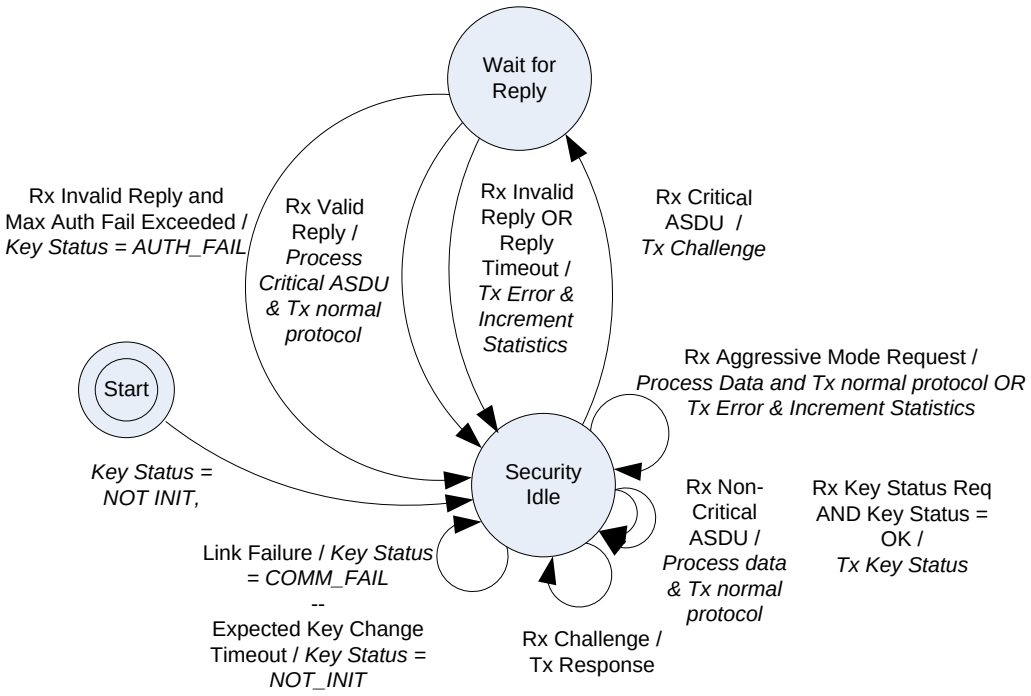


Figure 7-11: Major State Transitions for Outstation

7.5 Formal Specification

This subclause formally describes the protocol used for this authentication mechanism. If this subclause differs from 7.4, this subclause shall be considered to be definitive.

7.5.1 Message Definitions

This subclause describes the DNP3 messages used to implement the authentication mechanism. The DNP3 objects used are defined in Annex A.

7.5.1.1 Master Authentication Implementation

DNP3 masters shall implement the authentication mechanism using the function codes and objects described in Table 7-3. The first column of the table shows how these function codes and objects correspond to the IEC 62351-5 specification and the state machines in 7.5.2.

Table 7-3: DNP3 Master Messages with Correlation to IEC 62351-5

Shaded cells indicate optional messages

IEC 62351-5 Message	Description	Message From Master Contains		Outstation Responds With	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
Challenge	Requests authentication of the preceding outstation DNP3 Response or Unsolicited Response	0x20 Authentication Request	g120v1 Authentication Challenge object	0x83 Authentication Response	g120v2 Authentication Reply object
Reply	Provides authentication of a Challenge from the outstation	0x20 Authentication Request	g120v2 Authentication Reply object	0x81 Response If authentication was successful	Whatever objects are appropriate for the normal response to the master request that caused the outstation to issue the challenge
				0x83 Authentication Response If authentication failed	g120v7 Authentication Error object
Aggressive Mode Request	Provides authentication for the current DNP3 Request	Whatever function code is in the DNP3 Request	g120v3 Authentication Aggressive Mode Request object. Must be first object. • • • Objects appropriate for standard DNP3 request • • • g120v9 Authentication MAC object. Must be last object	0x81 Response If authentication was successful	Whatever objects are appropriate for the normal response to the master request
				0x83 Authentication Response If authentication failed	g120v7 Authentication Error object
Key Status Request	Requests the current status of the Session Keys.	0x20 Authentication Request	g120v4 Session Key Status Request object	0x83 Authentication Response	g120v5 Session Key Status object
Key Change	Changes the symmetric Session Keys subsequently used by master and outstation for authentication	0x20 Authentication Request	g120v6 Session Key Change object	0x83 Authentication Response	g120v5 Session Key Status object

IEC 62351-5 Message	Description	Message From Master Contains		Outstation Responds With	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
Error	Indicates the authentication provided in the challenge reply from outstation was incorrect or that the outstation's aggressive mode DNP3 response did not correctly authenticate	0x21 Authentication Request – No Ack	g120v7 Authentication Error object	None	None
User Status Change	The master informs the outstation that the authority has added or deleted a user or changed the information associated with a user	0x20 Authentication Request	g120v10 Authentication User Status Change OR g120v8 User Certificate	0x83 Authentication Response	None
				0x83 Authentication Response If the outstation could not validate the User Status Change using the authority's credentials	g120v7 Authentication Error object
Update Key Change Request	The master begins the process of changing the Update Key associated with a particular user by specifying the name of the user.	0x20 Authentication Request	g120v11 Authentication Update Key Change Request	0x83 Authentication Response	g120v12 Authentication Update Key Change Reply
				0x83 Authentication Response If Request is invalid	g120v7 Authentication Error object
Update Key Change Confirmation	Instead of actually changing the Update Key, the master may verify the outstation has the correct Update Key.	0x20 Authentication Request	g120v15 Update Key Change Confirmation (only)	0x83 Authentication Response	g120v15 Update Key Change Confirmation
				0x83 Authentication Response If authentication invalid	g120v7 Authentication Error object
Update Key Change	The master encrypts the new Update Key and sends it to the outstation, authenticating it	0x20 Authentication Request	g120v13 Update Key Change AND g120v14 Update Key Change	0x83 Authentication Response	g120v15 Update Key Change Confirmation

IEC 62351-5 Message	Description	Message From Master Contains		Outstation Responds With	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
	with either an asymmetric digital signature or a symmetric MAC.		Signature (asymmetric method) OR g120v15 Update Key Change Confirmation (symmetric method)	0x83 Authentication Response If authentication invalid	g120v7 Authentication Error object

7.5.1.2 Outstation Authentication Implementation

DNP3 outstations shall implement the authentication mechanism using the function codes, objects, and Internal Indications described in Table 7-4. The first column shows how they correspond to the IEC 62351-5 specification and the state machines in 7.5.2.

Table 7-4: DNP3 Outstation Messages with Correlation to IEC 62351-5

Shaded cells indicate optional messages

IEC 62351-5 Message	Description	Message From Outstation Contains		Message Initiated Because Master Sent	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
Challenge	Requests authentication of the preceding master DNP3 Request	0x83 Authentication Response	g120v1 Authentication Challenge object	Any valid function code	Whatever is appropriate to a solicited request
Request Secure Confirmation	Sends normal DNP3 data and requests the master to confirm it securely (using Aggressive Mode)	0x81 Response or 0x82 Unsolicited Response with CON bit set	Objects appropriate for standard DNP3 response • • • g120v1 Authentication Challenge object	Any valid request function code, or Master may not have sent anything but the Outstation sent an Unsolicited Response	Objects appropriate to the request, if the Master sent one
Reply	Provides authentication of a Challenge from the master	0x83 Authentication Response	g120v2 Authentication Reply object	0x20 Authentication Request	g120v1 Authentication Challenge object
Aggressive Mode Request	Provides authentication for the outstation's current DNP3 Response	0x81 Response or 0x82 Unsolicited Response	g120v3 Authentication Aggressive Mode Request object. Must be first object. • • • Objects appropriate for standard DNP3 response May also include Challenge Object as in "Request Secure Confirmation" • • • g120v9 Authentication MAC object. Must be last object	Any valid request function code, or Master may not have sent anything but the Outstation sent an Unsolicited Response	Objects appropriate to the request, if the Master sent one
Key Status	Response providing the outstation's current status of the Session Keys.	0x83 Authentication Response	g120v5 Session Key Status object	0x20 Authentication Request	g120v4 Session Key Status Request object

IEC 62351-5 Message	Description	Message From Outstation Contains		Message Initiated Because Master Sent	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
Key Change	Changes the symmetric Session Keys subsequently used by master and outstation for authentication	0x83 Authentication Response If authentication was successful	g120v5 Session Key Status object	0x20 Authentication Request	g120v6 Session Key Change object
		0x83 Authentication Response If authentication failed	g120v7 Authentication Error object		
User Status Change Response	Response indicating the outstation has received a User Status Change	0x83 Authentication Response If validation was successful	None	0x20 Authentication Request	g120v10 User Status Change OR g120v8 User Certificate
		0x83 Authentication Response If validation failed	g120v7 Authentication Error object		
Update Key Change Reply	Acknowledges that an Update Key is being changed and provides a User Number and random data to be used as part of the process.	0x83 Authentication Response If specified user exists	g120v12 Update Key Change Reply	0x20 Authentication Request	g120v11 Authentication Update Key Change Request
		0x83 Authentication Response If specified user does not exist	g120v7 Authentication Error object		
Update Key Change Confirmation	Confirms the new Update Key OR Verifies the current Update Key	0x83 Authentication Response If authentication was valid	g120v15 Update Key Change Confirmation	0x20 Authentication Request	g120v13 Update Key Change AND g120v14 Update Key Change Signature OR g120v15 Update Key Change Confirmation
		0x83 Authentication Response If authentication was invalid	g120v7 Authentication Error object		g120v15 Update Key Change Confirmation by itself

IEC 62351-5 Message	Description	Message From Outstation Contains		Message Initiated Because Master Sent	
		DNP3 Function Codes	DNP3 Objects	DNP3 Function Codes	DNP3 Objects
Error	Indicates authentication provided in the previous challenge reply from master was incorrect or that an aggressive mode request did not authenticate	0x83 Authentication Response If authentication failed	g120v7 Authentication Error object	0x20 Authentication Request	g120v2 Authentication Reply object
				Any valid function code	g120v3 Authentication Aggressive Mode Request object. • • • Objects appropriate for standard DNP3 request • • • g120v9 Authentication MAC object

7.5.1.3 DNP3 Sequence Numbering

Each DNP3 authentication Challenge, Reply or Error message shall have the same DNP3 application sequence number as the critical DNP3 fragment that was challenged.

Figure 7-12 illustrates how this rule would be applied for a Select/Operate control sequence using challenge and reply. DNP3 application sequence numbers are shown in parentheses. Figure 7-13 illustrates that when Aggressive Mode is used, the sequence numbering is identical to normal non-authenticated DNP3.

Implementers should note that the additional challenge and reply messages may require that certain timing parameters, such as the select-operate timeout, be increased.

Unless otherwise described in this subclause, normal DNP3 sequence numbering rules apply.

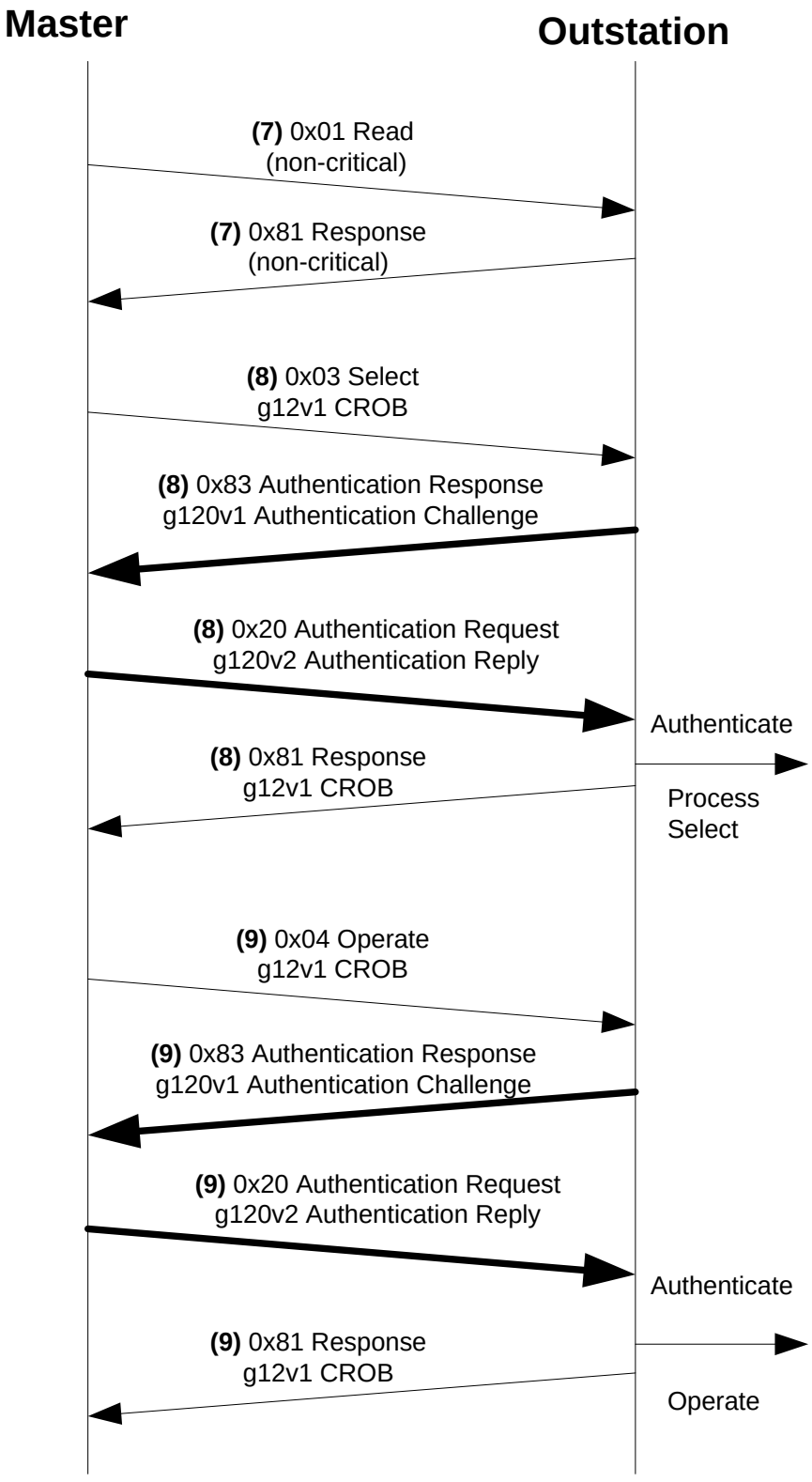


Figure 7-12: Example of DNP3 Select/Operate Authentication

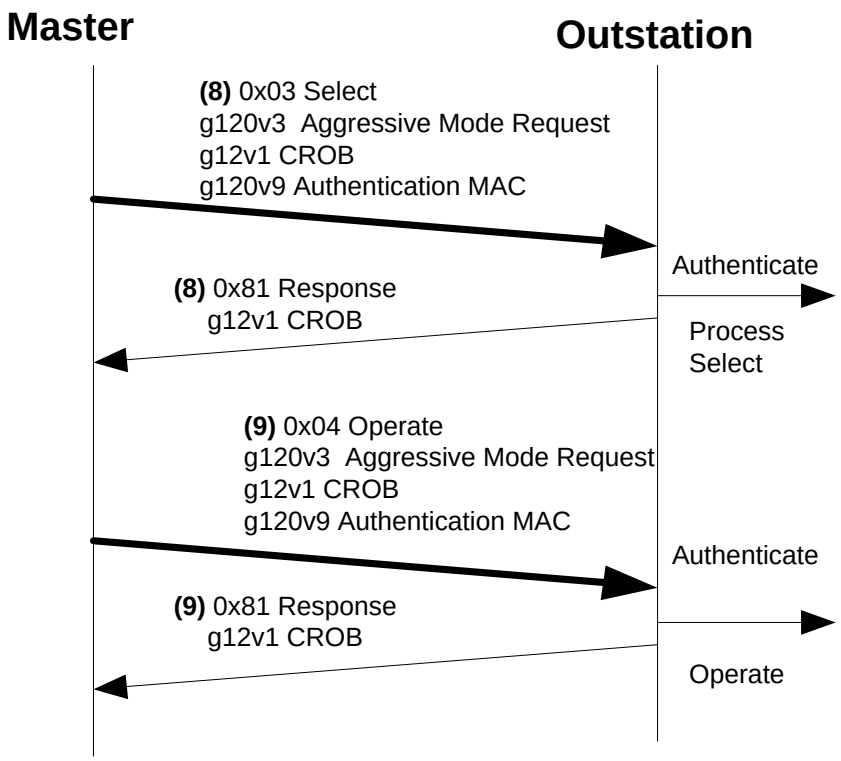


Figure 7-13 - Example of DNP3 Select/Operate Authentication in Aggressive Mode

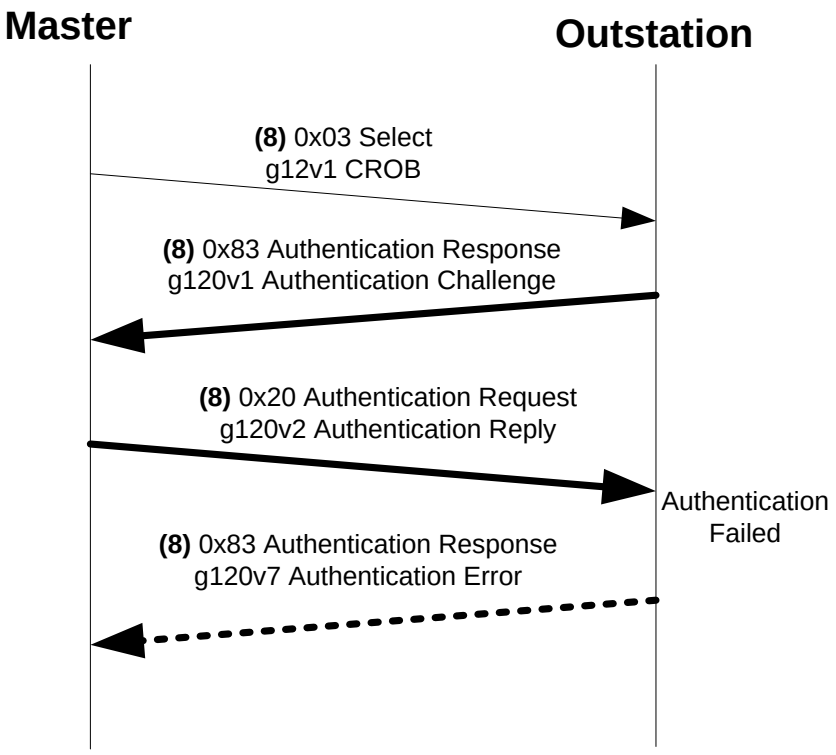


Figure 7-14: Example of Failed DNP3 Select/Operate Authentication

7.5.1.4 More DNP3 Message Examples

Figure 7-15 illustrates several of the messages described in the preceding subclauses as part of a typical initialization sequence. The outstation generates an unsolicited response to notify the master that it has restarted. Rather than confirm the unsolicited response, the master first initializes the Session Keys. Then, when the outstation re-attempts the restart unsolicited response, the master authenticates it before supplying a confirmation. The confirmation is not authenticated, but the outstation requires authentication of the Write operation. Following this sequence, both sides are permitted to use the Aggressive Mode because a complete challenge-reply sequence has taken place in both directions.

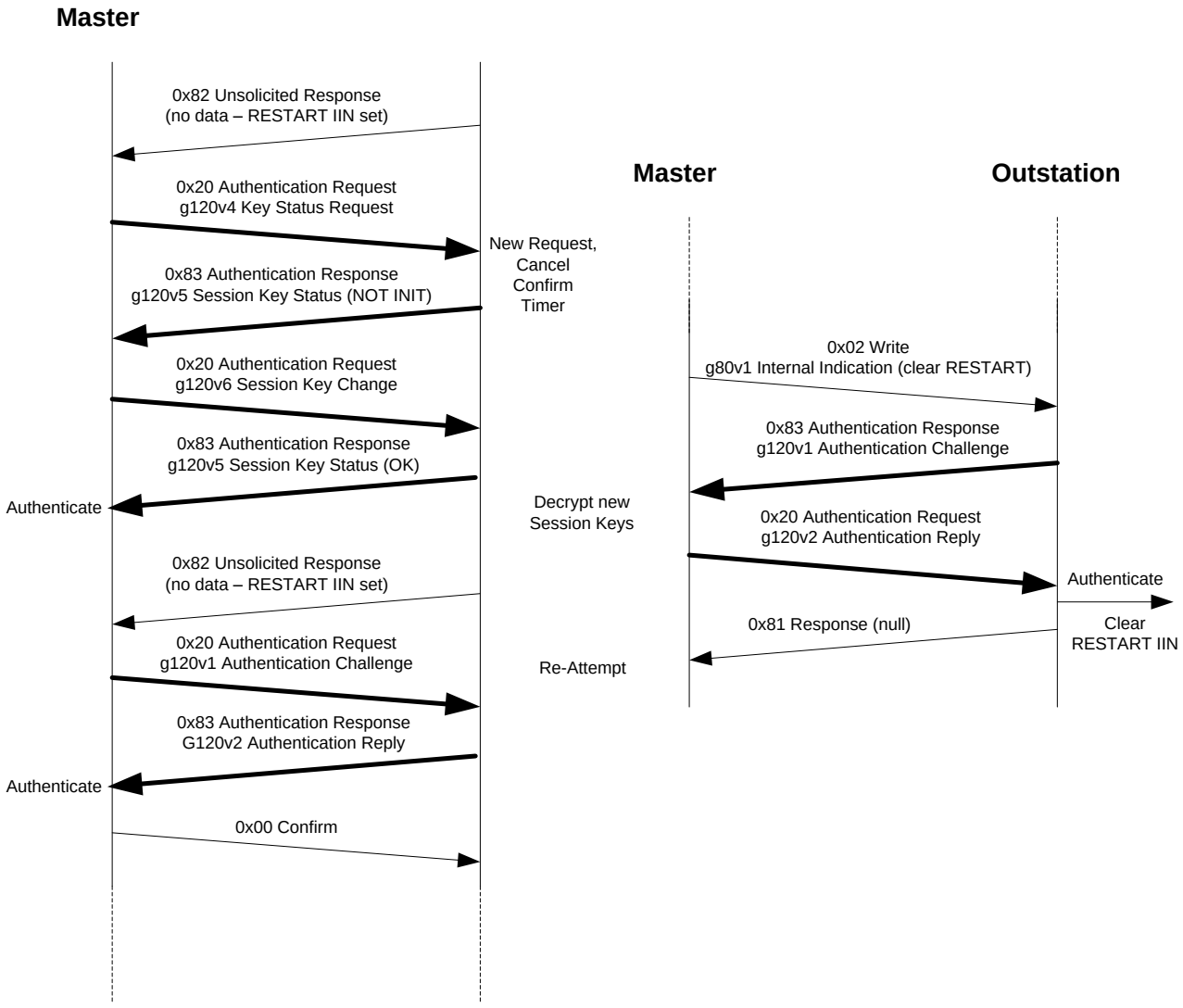


Figure 7-15: Example DNP3 Initialization Sequence

Figure 7-16 illustrates how a poll-response sequence could be authenticated in Aggressive Mode. The poll is not considered critical by the outstation, but the confirmation is. Since Responses and Confirms are optionally critical functions, it is up to the master to require that the Analog Change Events are critical, and up to the outstation to require that Confirms are critical.

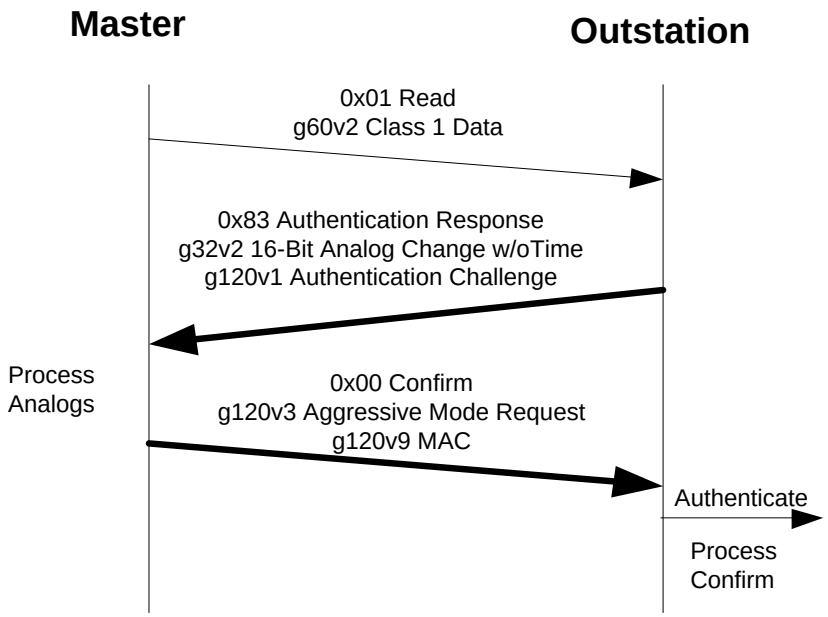


Figure 7-16: Example DNP3 Authentication of Outstation Polling Data

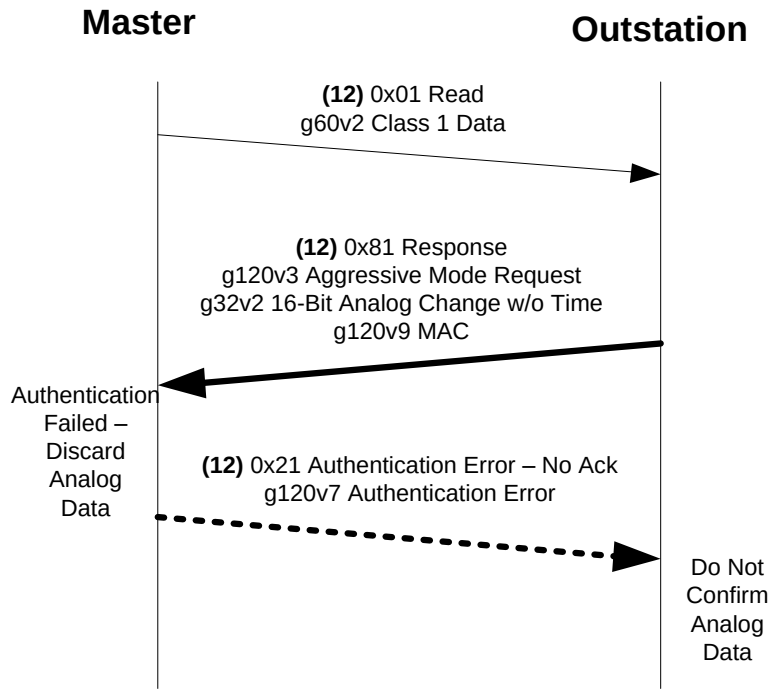


Figure 7-17: Example of Failed Authentication of Outstation Data

Figure 7-18 illustrates how the authority and a master would change a user's role (e.g. add the user or change the user's access permissions) and change the user's Update Key.

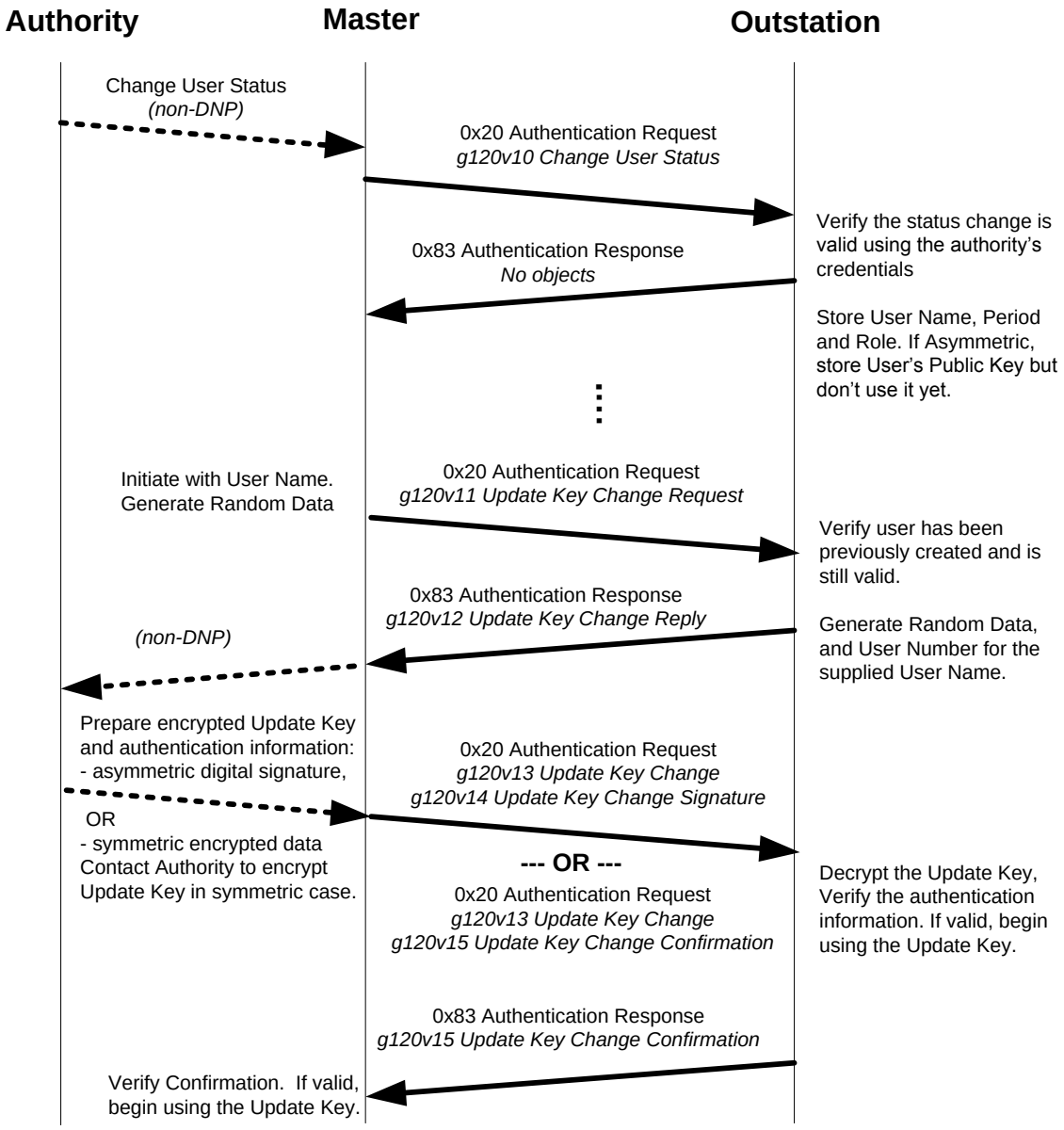


Figure 7-18 - Successful User Status Change and Update Key Change

Figure 7-19 illustrates how a user may change masters and continue communications with an outstation from a different location. Note that the data supplied by the user shall be provided in a secure manner but the details are out of the scope of this standard.

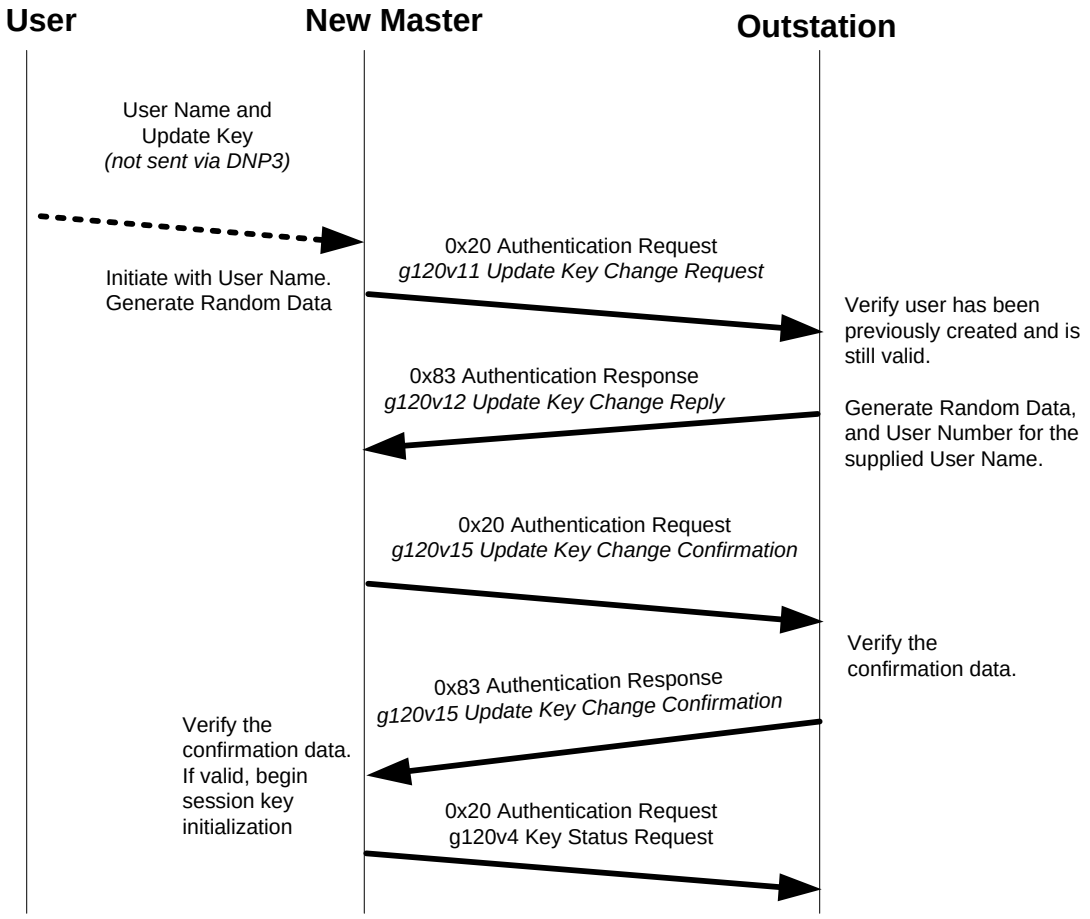


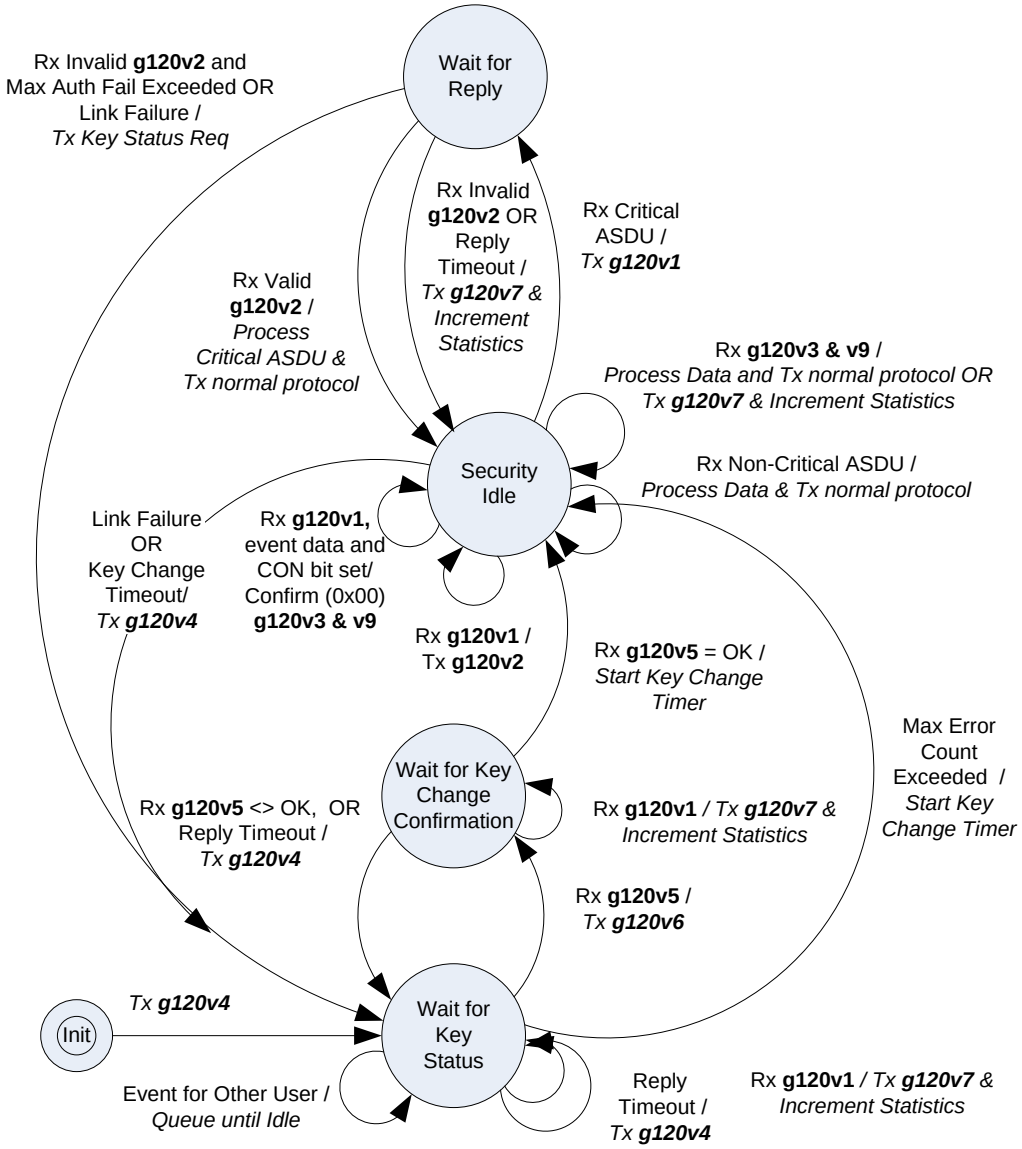
Figure 7-19: User Changes Masters

7.5.1.5 DNP State Machine Overviews

This subclause describes the state transitions in diagrams, using DNP3 function codes and object variations. These overview diagrams show only the major transitions; the tables in 7.5.2 are definitive.

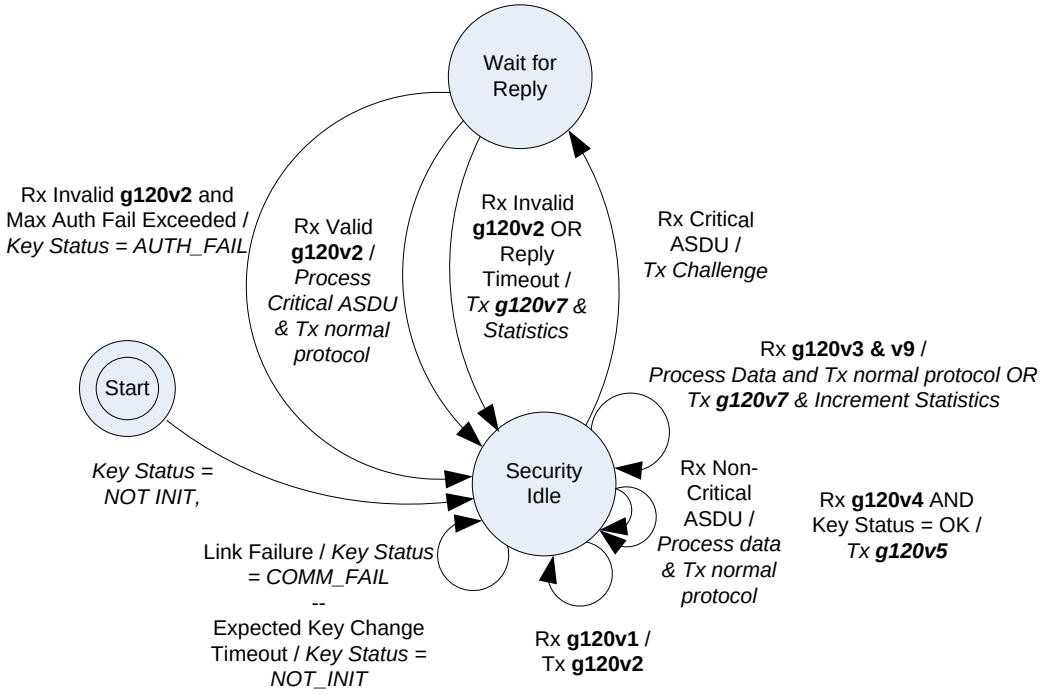
7.5.1.5.1 Authentication and Session Key Change State Machines

Figure 7-20 and Figure 7-21 are reproductions of Figure 7-10 and Figure 7-11 respectively, but with DNP3 function codes and object variations substituted for the authentication message names. They are provided here to illustrate how the IEC 62351-5 authentication mechanism is mapped to DNP3. Note that the top portion of the diagram remains the same for both master and outstation although the function codes used for transmitting and receiving the object variations are reversed.



Tx = Function Code **0x20** Authentication Request
Except **g120v7** uses **0x21** Authentication Request – No Ack
Rx = Function Code **0x83** Authentication Response if it is a security message

Figure 7-20: Master State Machine Showing DNP3 Function Codes and Object Variations

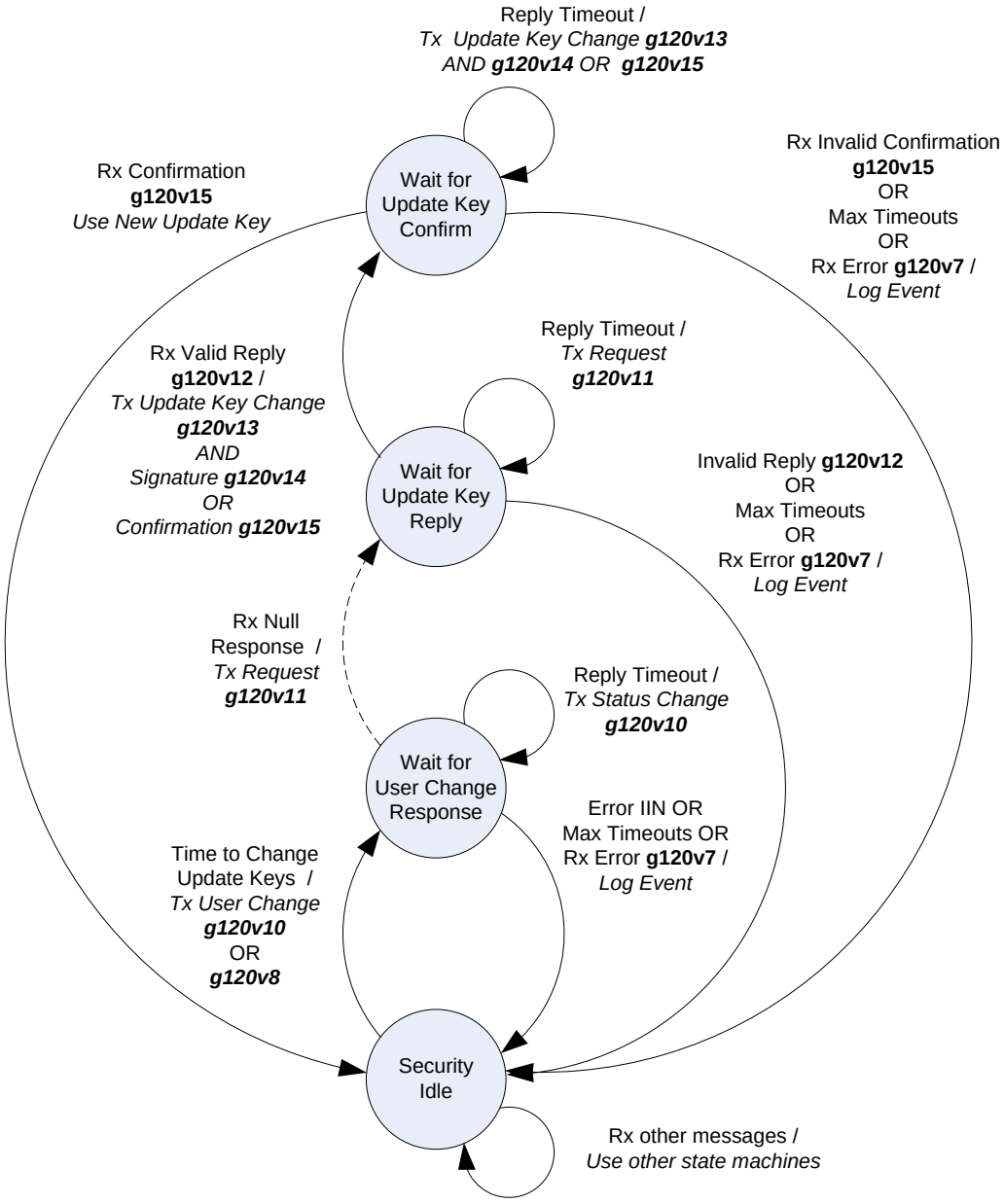


Tx = Function Code **0x83** Authentication Response
Rx = Function Code **0x20** Authentication Request if it is a security message

Figure 7-21: Outstation State Machine Showing DNP3 Function Codes and Object Variations

7.5.1.5.2 Update Key Change State Machines

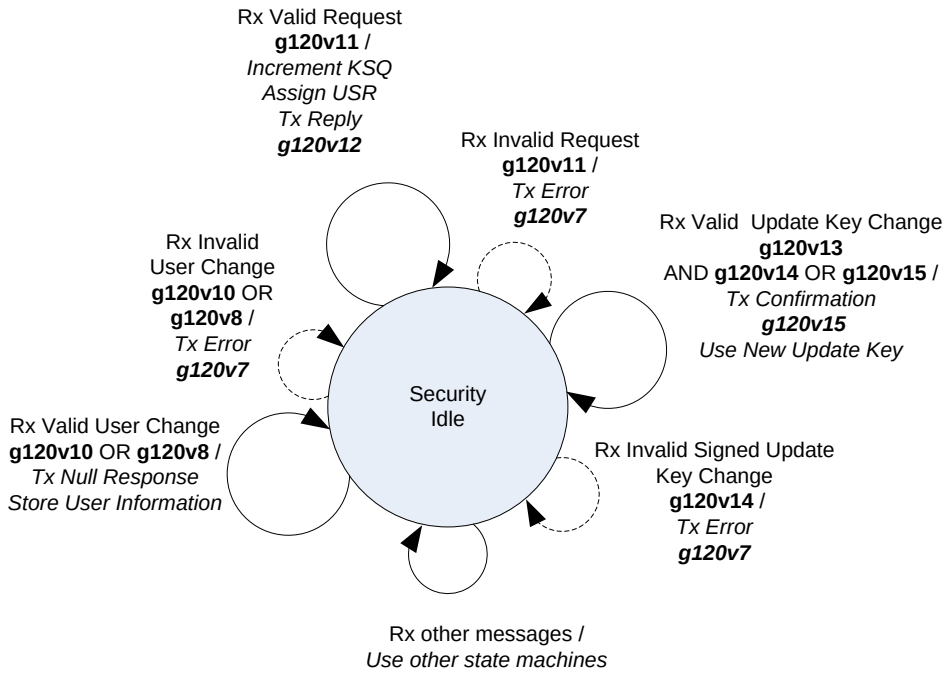
Figure 7-22 and Figure 7-23 illustrate the state machines for the master and outstation respectively when changing the status, role or Update Key of a user.



Tx = Function Code **0x20** Authentication Request
Rx = Function Code **0x83** Authentication Response

⇢ = Need not happen immediately; could return to Security Idle between these states

Figure 7-22: Master State Machine for Update Key Change



Tx = Function Code **0x83** Authentication Response
Rx = Function Code **0x20** Authentication Request
⇢ = Do not transmit Error (g120v7) if Max Error Count is exceeded

Figure 7-23: Outstation State Machine for Update Key Change

7.5.2 Formal Procedures

This subclause formally describes the procedures used by devices implementing this authentication mechanism as a part of each protocol. If this subclause differs from 7.4, this subclause shall be considered definitive.

The state machines in this subclause describe the protocol in terms of IEC 62351-5 “messages”. Refer to 7.5.1 for a description of how each of these messages is implemented using DNP3 function codes and objects, in each direction.

7.5.2.1 States

Table 7-5 describes the states used by these state machines, in the general order in which they might be expected to occur. Refer to 7.5.1.5 for an overview of how the state machines work together.

Table 7-5 - States Used in the State Machine Descriptions

State	Implemented in		Description	Refer to Table
	Master	Outstation		
Wait for Key Status	YES	No	The master has either just initialized, or its Session Keys have expired. It has just transmitted a Request Key Status message and is waiting for the outstation to transmit a Key Status message.	Table 7-13
Wait for Key Change Confirmation	YES	No	The master has transmitted a Key Change message and is waiting for the outstation to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK	Table 7-13
Wait for Reply	YES	YES	The Session Keys have been initialized and an authentication is in progress. One of the devices has transmitted a Challenge message and is waiting for the other end to transmit a Reply message. The critical ASDU that was challenged has been queued, waiting to be processed if the Reply is valid. It will be discarded if the Reply is invalid or an error condition occurs	Table 7-8
Security Idle	YES	YES	There is no authentication in progress. The device is executing the standard DNP3 protocol. The Session Keys may or may not be initialized.	Table 7-8
Wait for User Change Response	YES	No	The master has transmitted a User Status Change message and is waiting for the outstation to validate the Certification Data supplied by the authority indicating a change of status, role or Update Key for a user.	Table 7-14
Wait for Update Key Reply	YES	No	The master has transmitted an Update Key Change Request and is waiting for an Update Key Change Reply from the outstation.	Table 7-14
Wait for Update Key Confirm	YES	No	The master has transmitted a Update Key Change and is waiting for an Update Key Change Confirmation from the outstation.	Table 7-14

In each of these states except Security Idle, the device is waiting for a reply concerning a particular user. Devices shall keep a separate set of timers and states for each user. However, *only one user may be in a state other than Security Idle at a time.*

As illustrated in Figure 7-24 , if an event occurs in a state other than Security Idle, and the event concerns a user other than the one which entered that state, the device shall either queue the event or treat it as an error, as described in the state machines.

As an example of queuing, consider the case of initialization. If there are three users at the master, the master begins by sending a Request Key Status message for the first user and entering *Wait for Key Status* for that user. The initialization event for the other two users is queued by the master. The second user does not enter *Wait for Key Status* until the first user has reached *Security Idle* by either succeeding—or failing—to initialize its Session Keys.

As a different example, consider the case when an outstation is in *Wait for Reply* state waiting for User 1 to reply to a challenge, when the master unexpectedly sends a valid Aggressive Mode Request message for User 2. Per rows 15 through 17 of Table 7-8, the outstation stops waiting for the master to reply regarding User 1 and processes the request for User 2. The outstation does not process messages for two users at the same time.

Any events not covered by these state machines and procedures shall be ignored.

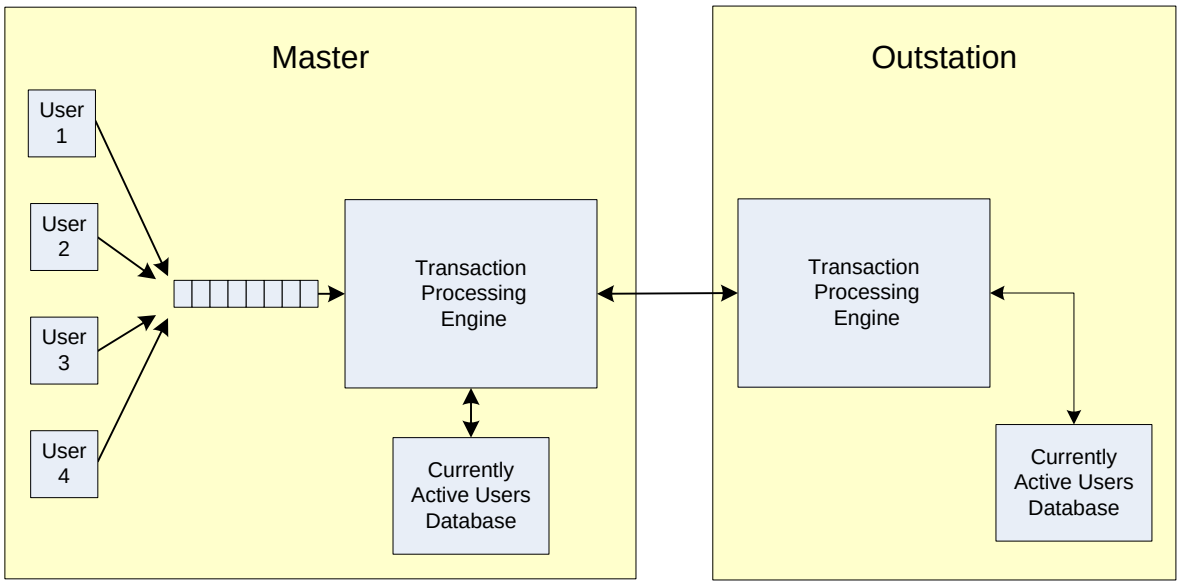


Figure 7-24: Behavior Model for Multiple Users

7.5.2.2 Security Statistics

DNP devices shall monitor the use of the Secure Authentication mechanism by counting a variety of protocol events. Outstations shall report the totals in DNP objects. Each DNP outstation that implements secure authentication shall report security statistics using the following objects:

- Security Statistic (g121v1)
- Security Statistic Change Event (g122v1)
- Security Statistic Change Event with Time (g122v2)

Table 7-6 lists the DNP indexes (point numbers) of each security statistic. They shall be the same for either group 121 (static) or group 122 (event) objects.

Each outstation shall maintain a local relative threshold for each statistic determining how often to report the statistic as an event object, as described in 7.6.1.4.2. In addition, the state machines shall use the following moving thresholds to determine when to react to error conditions:

- Max Authentication Failures
- Max Reply Timeouts
- Max Authentication Rekeys
- Max Error Messages Sent
- Max Rekeys Due to Restarts

Each time the state machine "resets" one of these Max values, it shall add the configured reporting threshold for that statistic to the current value of the statistic. Devices shall reset all the Max values at startup.

Table 7-6 summarizes the action to be taken for each statistic. The state machine tables describe the precise conditions under which the statistics are to be incremented, and the specific actions to be taken. The exception is the Total Messages Sent and Total Messages received, which are incremented too frequently to be documented specifically.

An outstation may report Security Statistic objects on DNP associations other than the one the statistics are measuring. This practice permits a master to detect a potential attack on a different DNP association by monitoring that association's statistics.

Each statistic object shall contain its Association ID. An association ID of 0 shall indicate the statistic is being reported on the same association it is measuring.

The following rules apply regarding statistics reporting on multiple associations.

a) Each association shall report its "own" statistics as points 0 to "n-1", where "n" is the number of standard statistics listed in Table 7-6. In this version of the specification, "n" is 18.

b) Statistics for any other associations shall be allocated in blocks of "n" points at the discretion of the outstation. The DNP indexes listed in Table 7-6 become offsets within these blocks. For instance, the second set of statistics reported by an outstation (if it chooses to report more than one set) are always points "n" to "2n – 1"

c) Masters must therefore know what "n" is for any given version of the protocol, based on the Device Attribute variation 210 indicating the number of security statistics.

d) The combination of the Association ID and the point number modulo "n" will always uniquely identify the statistic within the outstation.

e) Association IDs are not necessarily sequential or follow any other pattern. They simply allow the outstation to uniquely identify the association.

Table 7-6: Indexes of Security Statistics Objects

Index	Name	Increment whenever…	Default Threshold	Additional Action
0.	Unexpected Messages	The other device has responded with a message that was not the expected next step in the state machine.	3	Log each occurrence.
1.	Authorization Failures	The other device has replied with the correct authentication information, so the user is authentic, but the user is not authorized to perform the requested operation.	5	Log each occurrence.
2.	Authentication Failures	The other device has provided invalid authentication information such as an incorrect MAC.	5	If **Max Authentication Failures** has been exceeded, change session keys and increment the Rekeys Due to Authentication Failure.
3.	Reply Timeouts	The other device has not replied within the configured time required as described in 7.6.1.4.1.	3	If **Max Reply Timeouts** has been exceeded, cancel the current transaction.
4.	Rekeys Due to Authentication Failure	An Authentication Failure has occurred that causes the master station to change the session keys (i.e. the Authentication Failure threshold was exceeded	3	If **Max Authentication Rekeys** has been exceeded, stop changing session keys due to Authentication Failures. Start changing keys due to Authentication Failures again only if they are first changed successfully for other reasons.
5.	Total Messages Sent	The device sends a DNP application layer fragment.	100	None.
6.	Total Messages Received	The device receives a DNP application layer fragment.	100	None.
7.	Critical Messages Sent	The device receives a Challenge message or transmits an Aggressive Mode Request message.	100	None.
8.	Critical Messages Received	The device transmits a Challenge message or receives an Aggressive Mode Request message.	100	None.
9.	Discarded Messages	The device discards a received message.	10	None.
10.	Error Messages Sent	The device has sent a fragment containing an Error object indicating an authentication failure or potential configuration error.	2	If **Max Error Messages Sent** has been exceeded, stop sending Error objects. Start sending Error objects again only if session keys are successfully changed.
11.	Error Messages Rxed	The device has received an Error object	10	None.
12.	Successful Authentications	The device successfully authenticates a message.	100	None.
13.	Session Key Changes	A user successfully changes session keys.	10	None.

Index	Name	Increment whenever…	Default Threshold	Additional Action
14.	Failed Session Key Changes	A user fails to change session keys	5	None.
15.	Update Key Changes	The master and authority change the Update Key for a user.	1	None.
16.	Failed Update Key Changes	The master and authority fail to change the Update Key for a user.	1	None.
17.	Rekeys Due to Restarts	Only used by a master. Set to zero in outstations. The master rekeyed the session keys because the outstation restarted.	3	If **Max Rekeys Due to Restarts** has been exceeded, stop changing session keys due to outstation restarts until the next Key Change Timeout.

7.5.2.3 Challenger procedures

7.5.2.3.1 Challenger Role

A device, either master or outstation, that requires authentication from the other device in order to communicate, shall be called a Challenger. Challengers shall issue Challenge messages in reply to Critical ASDUs, according to the state machine described in Table 7-8.

The Challenger shall calculate pseudo-random Challenge Data according to FIPS 186-2 and include it in the Challenge message.

Challengers shall never intentionally retransmit the same Challenge message. Any time a Challenge is issued, it shall be created using new Challenge Data and a new Challenge Sequence Number.

Note that in order to reach either of the two states described in Table 7-8, the Challenger must have established a set of Session Keys using the Master state machine in Table 7-13.

Each fragment of a multi-fragment Response shall be challenged individually. If a master issues a challenge to a multi-fragment response (function codes 129 or 130) from an outstation, it shall issue a challenge for each fragment in the response.

The CON (confirm) bit is never set in Authentication Response fragments transmitted by the outstation unless multiple fragments are sent, or an aggressive mode confirmation is requested by sending an Authentication Challenge with the CON bit set, as described in 7.5.2.3.2.

7.5.2.3.2 Critical Functions

Each Challenger shall distinguish between Critical ASDUs and Non-Critical ASDUs. A Critical ASDU shall be a message implementing a function that the Challenger requires to be authenticated. IEC 62351-5 states the following minimum requirements:

- *Outstations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical.*
- *Challengers may optionally consider additional functions beyond this minimum subset to be critical.*

The following rules are used to identify the DNP3 operations that shall be considered critical, requiring authentication.

a) Any application layer DNP3 Requests identified with a "MANDATORY" in the "Critical" column of Table 7-7 shall be considered critical operations. DNP3 outstations complying with this authentication mechanism shall require masters to authenticate all DNP3 Request fragments that contain these function codes.

a) DNP3 outstations may optionally require authentication of any other Request fragments.

b) There are no DNP3 Responses that are mandatory for a DNP3 master to designate as critical operations. DNP3 masters may optionally require authentication of any DNP3 Response, but are not required to do so for compliance.

c) If a DNP3 device claims compliance with this authentication mechanism, information identifying those function-codes and objects the device considers critical, requiring authentication, shall accompany the Device Profile Document for the device.

d) Implementers of outstations should note that if an outstation considers Confirm (0x00) function codes to be critical and issues a challenge, the master may not be expecting the message. On half-duplex or multi-drop links, it is possible that the challenge would collide with the master's next request as shown in Figure 7-25. Outstations that wish to consider confirmations critical shall include an Authentication Challenge object (g120v1) following the regular DNP3 data in the response to be confirmed, as shown in Figure 7-26. Master stations receiving a response with the CON bit set and an Authentication Challenge object included shall issue the confirmation in aggressive mode.

e) Note that this case is an exception to the rule that a complete Challenge-Reply must be completed before aggressive mode can be used. There is sufficient information in the Challenge object to create the aggressive mode MAC, and the aggressive mode confirmation therefore essentially constitutes a Reply.

f) If an outstation wishes to send an aggressive mode response or unsolicited response *and* wishes the master to send the confirmation in aggressive mode, the Authentication Challenge object (g120v1) shall be the *second-last* object and the Authentication MAC (g120v9) shall be the *last* object. Refer to Table 7-4 for more details.

g) An outstation shall not send an Authentication Challenge object (g120v1) in the initial NULL unsolicited response after a restart.

h) A similar problem may occur if a master sends any of the following function codes:

   1) Direct Operate – No Acknowledgement (0x06)

   2) Immediate Freeze – No Acknowledgement (0x08)

   3) Freeze-and-Clear – No Acknowledgement (0x0A)

   4) Freeze-at-Time – No Acknowledgement (0x0C)

   When sending one of these function codes, a master shall either:

   — Wait to see if the outstation challenges them before proceeding OR

   — Send them only in aggressive mode.

i) Any device may arbitrarily decide that a fragment is critical and can therefore initiate a challenge for any reason. The burden is on the replying station to process the challenge regardless of whether it is expected.

j) Any messages capable of changing security configuration parameters shall be considered critical.

k) An outstation receiving a properly authenticated message that is intended to cause a restart (e.g. Warm Restart, Cold Restart, Activate Configuration) may send a response to the master and restart without waiting to discover whether the response was challenged by the master. A master is therefore not required to challenge such a response even if responses (function code 129) are generally considered critical.

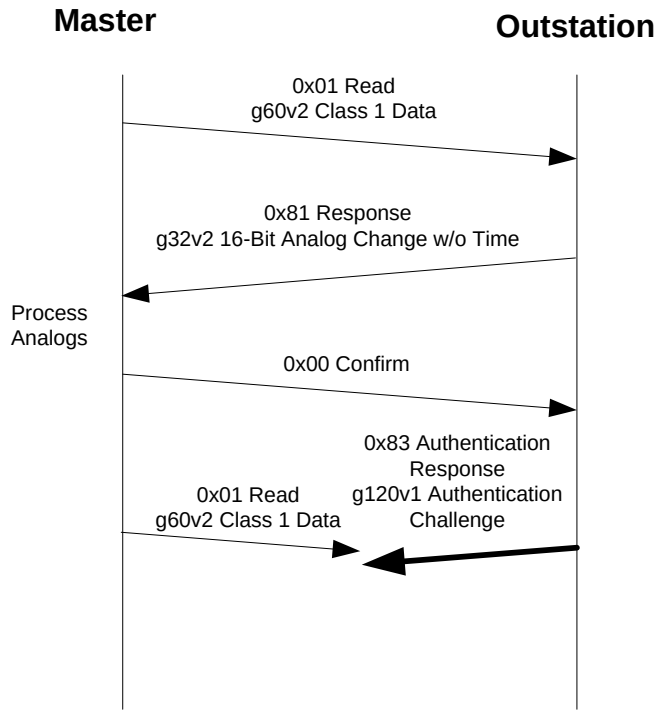


Figure 7-25: Possible Collision of Confirmation Challenge and Next Master Request

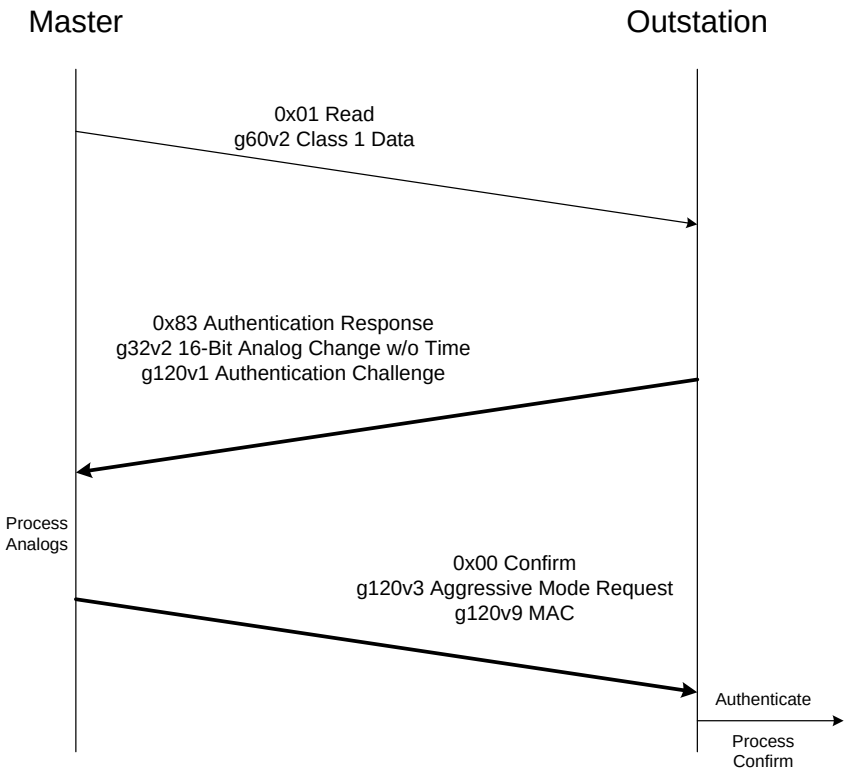


Figure 7-26: Preventing Confirmation Challenge Collisions Using Aggressive Mode

Table 7-7: DNP3 Critical Request Function Codes

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 (new)	Not applicable
33	0x21	Authentication Request – No Ack (new)	Not applicable
129	0x81	Response	optional
130	0x82	Unsolicited Response	optional
131	0x83	Authentication Response (new)	Not applicable

7.5.2.3.3 Use of Challenge Sequence Numbers

Challengers and Responders shall maintain a Challenge Sequence Number (CSQ) between them to match Replies with Challenges, according to the following rules:

a) Devices shall set their CSQ to zero on startup.

b) Devices shall increment the CSQ each time they transmit a Challenge message.

c) Devices shall set the CSQ of each Reply message to that of the most recently received Challenge message.

d) Devices shall set the CSQ of each Reply or Aggressive Mode Request message to that of the most recently received Challenge message, plus the number of Aggressive Mode Request messages or Reply messages the device has transmitted since receiving the Challenge message. Note that rule c) is a special case of rule d).

e) A device that receives an Aggressive Mode Request message with a valid MAC shall set the CSQ in its next outgoing Challenge message to that found in the Aggressive Mode Request message plus one, unless either:

    1) The MAC on the Aggressive Mode Request is invalid.

    2) The resulting CSQ would be smaller than the one the device would have sent normally.

f) If the value of the CSQ reaches 4294967295, the next time a device increments the CSQ it shall become zero.

g) Challenge sequence numbers shall be independent of User Number. In other words, each device need only store a single value of CSQ locally *for each direction*, regardless of how many users it is communicating with.

h) Devices using unsolicited responses shall maintain two sets of Challenge data, one for Challenges sent in DNP3 responses and one for Challenges sent in DNP3 unsolicited responses.

Examples of the effect of these rules are illustrated in Figure 7-27 and Figure 7-28. The notation "Data=A", "Data=B", etc. indicates when the outstation changes the Challenge Data and which instance of this data the master uses to construct its Reply or Aggressive Mode Request.

Figure 7-27 illustrates a simple case in which a Challenge-Reply sequence is followed by two Aggressive Mode Requests. The CSQ of the Reply matches the Challenge, and the CSQ of each Aggressive Mode Request increments thereafter. The same Challenge Data from the original Reply is used for all transactions.

Figure 7-28 illustrates a much more complex case. Following the sequence in Figure 7-27, the outstation sends an unsolicited response at the same time the master requests a critical operation. The messages cross in transit and the devices must use the CSQs to match transactions. In the middle of this example, the outstation has two Challenges outstanding, one with CSQ=4 and Data=B, and the other with CSQ=5 and Data=C.

Following the example in Figure 7-28, one of the following cases may occur depending on what happens first:

— If the master sends an Aggressive Mode Request, it will do so with CSQ=6 and Data=C, the last Challenge Data it received.

— If the master sends a critical ASDU and the outstation challenges it, the new Challenge will contain CSQ=6 and new Data=D.

— If the outstation sends an unsolicited response containing a Challenge, the new Challenge will also contain CSQ=6 and new Data=D.

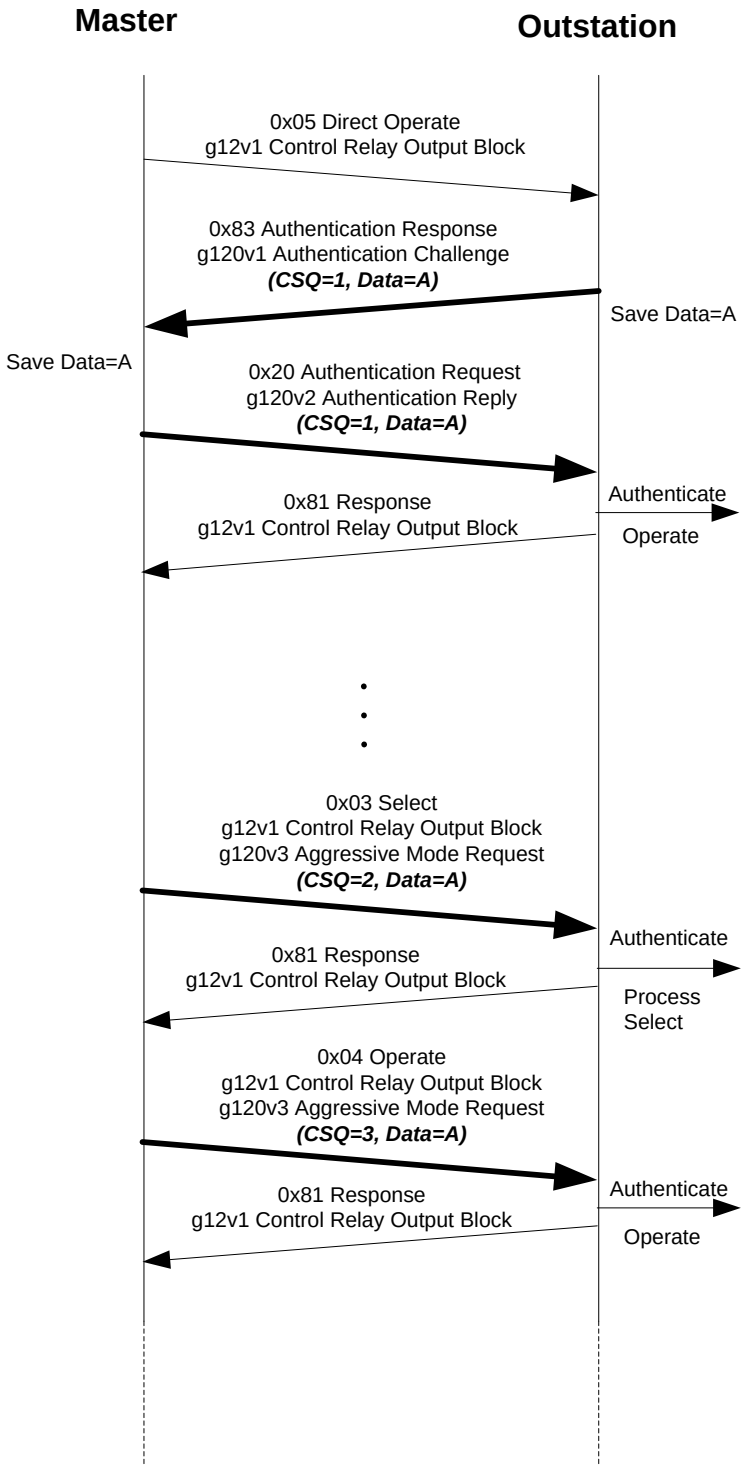


Figure 7-27: Example Use of Challenge Sequence Numbers (part 1)

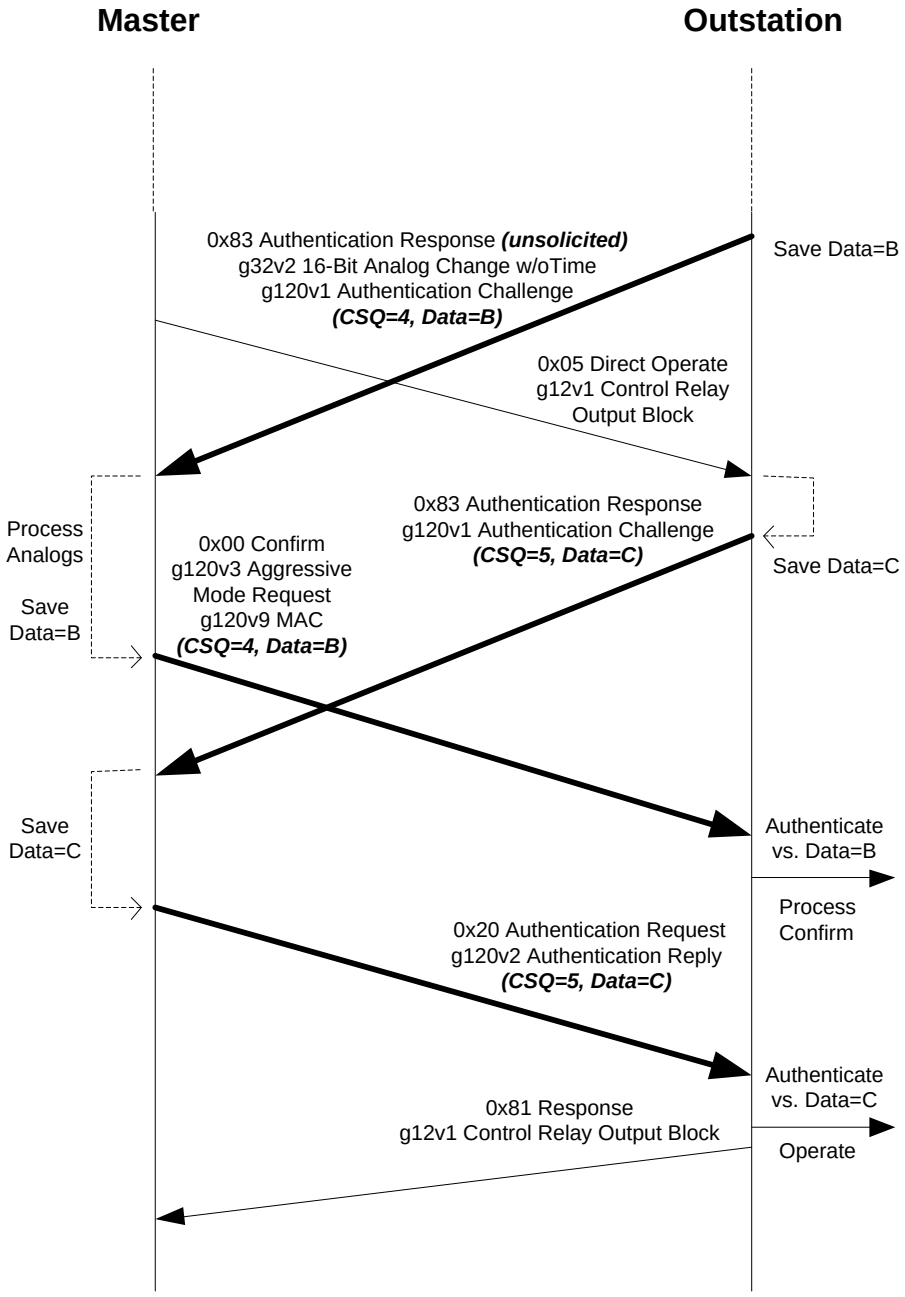


Figure 7-28: Example Use of Challenge Sequence Numbers (part 2)

7.5.2.3.4 Authentication Procedures

If the Challenger is in the states *Wait for Key Status*, or *Wait for Key Change Confirmation*, when it receives a Reply message, it shall consider the Reply message to be an *Rx Invalid Reply* event because the Session Keys are not valid. Similarly, if the Challenger receives an Aggressive Mode Request in any of these states, the Challenger shall consider it to be an *Rx Invalid Aggressive Mode Request* event.

Upon receiving a Reply message, the Challenger shall calculate the MAC Value from the information it transmitted in the Challenge message, as described in the definition of the Authentication Challenge object.

If the MAC Value from the Reply matches the calculated MAC Value, and the Challenge Sequence Numbers from the Challenge and Reply messages also match, the Challenger shall consider the Reply message to be a *Rx Valid Reply* event.

Otherwise, the Challenger shall consider the Reply message to be an *Rx Invalid Reply* event.

Upon receiving an ASDU containing an Aggressive Mode Request, the Challenger shall calculate the MAC Value from the information in the ASDU as described in the definition of the Authentication Aggressive Mode Request object. If the MAC Value in the Aggressive Mode Request matches the calculated MAC Value and the Challenge Sequence Number in the Aggressive Mode Request is correct as described in the definition of the Authentication Aggressive Mode Request object, the Challenger shall consider the ASDU to be a *Rx Valid Aggressive Mode Request* event.

Otherwise, the Challenger shall consider the Aggressive Mode Request message to be an *Rx Invalid Aggressive Mode Request* event.

In particular, the Challenger shall consider any Aggressive Mode Request to be an *Rx Invalid Aggressive Mode Request* event if the Challenger has not previously received at least one *Rx Valid Reply* event from the Responder. This rule follows from the definition of the Aggressive Mode Request, because the Challenge Sequence Number in an Aggressive Mode Request is derived from the Challenge Sequence Number found in the Challenge most recently received by the Responder.

7.5.2.3.1 Challenger State Machine

Challengers (either master or outstation) shall implement the state machine described in Table 7-8. Note that whenever the outstation sets the Key Status to a value other than OK, the set of Session Keys for the identified user shall be considered invalid and all authentication attempts for that user shall fail until the Key Status is OK again.

Table 7-8: Challenger State Machine

Event	Event Description	State				
		Security Idle		**Wait for Reply**		
		The device is executing the standard DNP3 protocol.		**The device is waiting for the other device to authenticate itself.**		
		Action	**Next State**	**Action**	**Next State**	
A	B	C	D	E	F	
Rx Unsolicited Non-Critical ASDU	MASTER ONLY. The master receives an unsolicited ASDU that does not require authentication.	Process the ASDU and issue a Confirm.	Security Idle	Process the ASDU and issue a Confirm.	Wait for Reply	1
Rx Non-Critical ASDU	The Challenger receives an ASDU that does not require authentication.	Process the Non-Critical ASDU and transmit any appropriate response required by the standard protocol.	Security Idle	Increment the Unexpected Messages statistic. Log the occurrence. Discard the new Non-Critical ASDU. Increment the Discarded Messages statistic.	Wait for Reply	2
Rx Critical ASDU	The Challenger receives an ASDU that requires authentication.	If (MASTER and Session Keys are valid) OR If OUTSTATION: Increment the Challenge Sequence Number (CSQ). Create and transmit a Challenge message calculated from the Critical ASDU. Start the Reply Timer. Queue the Critical ASDU for execution later. Increment the Critical Messages Received statistic	Wait for Reply	Increment the Critical Messages Received statistic Increment the Unexpected Messages statistic. Log the occurrence. Discard the new Critical ASDU. Increment the Discarded Messages statistic.	Wait for Reply	3

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
		If MASTER and Session Keys are Invalid: Transmit a Key Status Request Message. Start the Reply Timer. Increment the Critical Messages Received statistic	Wait for Key Status (Table 7-13)		Wait for Reply	4
Rx Valid Reply	The Challenger receives a Reply message that correctly authenticates the other device based on the most recently transmitted Challenge.	Discard the message. Increment the Unexpected Messages statistic. Log the occurrence. Increment the Discarded Messages statistic.	Security Idle	If a critical ASDU is queued awaiting the challenge response, then process the ASDU and transmit the ASDU's response. Cancel the Reply Timer. Reset Max Reply Timeouts. Increment the Successful Authentications statistic.	Security Idle	5
Rx Invalid Reply	The Challenger receives a Reply message that does not correctly authenticate the other device.	Discard the message. Increment the Unexpected Messages statistic. Log the occurrence. Increment the Discarded Messages statistic.	Security Idle	Increment the Authentication Failures statistic Cancel the Reply Timer. Reset Max Reply Timeouts. Discard the ASDU that was queued pending authentication. Increment the Discarded Messages statistic. If the Max Error Messages Sent has not been exceeded, transmit an Error Message with reason <1> Authentication Failed. If the Max Authentication Failures has been exceeded, behave according to the "Max Authentication Failures Exceeded" event below.	Security Idle	6

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Reply Timeout	The Reply Timer started when entering Wait for Reply state has expired. This may be the standard response timer for the protocol. Refer to 7.6.1.4.1 for details regarding the Reply Timer.	Should not occur – this is an error condition.	Security Idle	Increment the Reply Timeouts statistic. Cancel the Reply Timer. Discard any ASDUs that were queued pending an authentication Reply. Increment the Discarded Messages statistic	Security Idle	7
Max Reply Timeouts Exceeded Or Comm Failure Detected	• The Reply Timeouts statistic has exceeded Max Reply Timeouts • The protocol has detected a communications failure for some other reason. This event affects all users. Refer to 7.6.1.4.1 for details regarding the Reply Timer.	MASTER: Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 7-13)	MASTER: Discard the critical ASDU that was queued pending authentication. Increment the Discarded Messages statistic. Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 7-13)	8
		OUTSTATION: Set the current Key Status to COMM_FAIL. Reset Max Reply Timeouts.	Security Idle	OUTSTATION: Discard the critical ASDU that was queued pending authentication. Increment the Discarded Messages statistic. Set the current Key Status to COMM_FAIL Reset Max Reply Timeouts.	Security Idle	9

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Max Authentication Failures Exceeded	The Authentication Failures statistic has exceeded Max Authentication Failures. This may be due to a Rx Invalid Reply event, or a Rx Invalid Aggressive Mode Request event.	MASTER: IF the Rekeys Due to Authentication Failure statistic is <= Max Authentication Rekeys Transmit a Key Status Request Message. Start the Reply Timer. Increment the Rekeys Due To Authentication Failure statistic. Reset Max Authentication Failures	Wait for Key Status (Table 7-13)	MASTER: IF the Rekeys Due to Authentication Failure statistic is <= Max Authentication Rekeys Transmit a Key Status Request Message. Start the Reply Timer. Increment the Rekeys Due To Authentication Failure statistic. Reset Max Authentication Failures Discard the pending Critical ASDU Increment Discarded Messages statistic.	Wait for Key Status (Table 7-13)	10
		MASTER or OUTSTATION IF Rekeys Due to Authentication Failure statistic is > Max Authentication Rekeys Reset Max Authentication Failures IF operating over TCP Close TCP connection Log the event	Security Idle	MASTER or OUTSTATION: IF Rekeys Due to Authentication Failure statistic is > Max Authentication Rekeys Reset Max Authentication Failures IF operating over TCP Close TCP connection Log the event	Security Idle	11
		OUTSTATION: IF the Rekeys Due to Authentication Failure statistic is <= Max Authentication Rekeys Set the current Key Status to AUTH_FAIL. Increment the Rekeys Due To Authentication Failure statistic. Reset Max Authentication Failures	Security Idle	OUTSTATION: IF the Rekeys Due to Authentication Failure statistic is <= Max Authentication Rekeys Set the current Key Status to AUTH_FAIL. Increment the Rekeys Due To Authentication Failure statistic. Reset Max Authentication Failures Discard the pending Critical ASDU Increment Discarded Messages statistic.	Security Idle	12

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Error Message	The Challenger receives an Error Message.	Log the Error message, noting that the message was unexpected. Increment the Error Messages Rxed statistic.	Security Idle	Log the error message. If the Error Code is <5> MAC algorithm Not Permitted, use a different MAC algorithm to send the next Challenge. Do not send another Challenge immediately, but wait for an appropriate event to cause the Challenge. Discard the pending ASDU. Increment the Discarded Messages statistic. Increment the Error Messages Rxed statistic. Cancel the Reply Timer. Reset Max Reply Timeouts.	Security Idle	13
Key Change Timeout	For MASTER only. Either the Key Change timer has expired, or The Key Change Count has been exceeded. Refer to 7.6.1.4.	Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Rekeys Due to Restarts	Wait for Key Status (Table 7-13)	Queue the event and process it after returning to Security Idle state.	Wait for Reply	14
Expected Key Change Timeout	For OUTSTATION only. The outstation has not received a valid Key Change message within the Session Key Change interval or Session Key Change count configured at the outstation. Refer to 7.6.1.4.	Set Key Status = NOT_INIT for the user specified in the timeout. Invalidate those session keys.	Security Idle	Set Key Status = NOT_INIT for the user specified in the timeout. Invalidate those session keys.	Wait for Reply	15

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Key Status Request	For OUTSTATION only. The outstation receives a Key Status Request message.	IF USR is valid Transmit a Key Status message containing the current Key Status. ELSE Increment the Unexpected Messages statistic. Discard the Key Status Request Increment the Discarded Messages statistic.	Security Idle	Increment the Unexpected Messages statistic. Discard the Key Status Request Increment the Discarded Messages statistic.	Wait for Reply	16
Rx Valid Aggressive Mode Request	The Challenger receives an ASDU containing an Aggressive Mode Request message that correctly authenticates the other device.	IF Aggressive Mode is enabled: Perform the operations specified in the ASDU containing the Aggressive Mode Request and transmit any appropriate response required by the standard protocol. Increment the Successful Authentications statistic.	Security Idle	IF Aggressive Mode is enabled for OUTSTATION and the Aggressive Mode Request is not an application layer Confirm: Discard the previously pending Critical ASDU. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic. Perform the operations specified in the ASDU containing the Aggressive Mode Request and transmit any appropriate response required by the standard protocol. Increment the Successful Authentications statistic. Cancel the Reply Timer. Reset Max Reply Timeouts.	Security Idle	17

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
				IF Aggressive Mode is enabled for OUTSTATION and the Aggressive Mode Request is an application layer Confirm: Process the Aggressive Mode Request, e.g. release buffered events as appropriate Increment the Successful Authentications statistic	Wait for Reply	18
				IF Aggressive Mode is enabled for MASTER Process the Aggressive Mode Request and send Confirm if appropriate Increment the Successful Authentications statistic	Wait for Reply	19
		IF Aggressive Mode is disabled: Discard the Aggressive Mode request. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Security Idle	IF Aggressive mode is disabled, Discard the Aggressive Mode Request. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for Reply	20

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
		IF the Error Messages Sent statistic is <= Max Error Messages Sent,, transmit an Error Message with reason <2> Aggressive Mode Not Supported.		If Aggressive mode is disabled AND the Error Messages Sent statistic is <= Max Error Messages Sent, In addition to the steps above, Discard the pending critical ASDU. Increment the Discarded Messages statistic. Transmit an Error Message with reason <4> Aggressive Mode Not Supported. Cancel the Reply Timer. Reset Max Reply Timeouts.	Security Idle	21
Rx Invalid Aggressive Mode Request	The Challenger receives an ASDU containing an Aggressive Mode Request that does not correctly authenticate the other device. Note that all Aggressive Mode Requests are invalid until at least one valid challenge reply has been received.	IF aggressive mode is enabled, Increment the Authentication Failures statistic. IF the Error Messages Sent statistic is <= Max Error Messages Sent Transmit an Error Message with reason <1> Authentication Failed.	Security Idle	IF aggressive mode is enabled, Increment the Authentication Failures statistic. Increment the Unexpected Messages statistic. Discard the Aggressive Mode Request. Increment the Discarded Messages statistic.	Wait for Reply	22

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
		IF aggressive mode is disabled, Discard the Aggressive Mode Request. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic. IF the Error Messages Sent statistic is <= Max Error Messages Sent,, Transmit an Error Message with reason <2> Aggressive Mode Not Supported.	Security Idle	IF aggressive mode is disabled, Increment the Unexpected Messages statistic. Discard the Aggressive Mode Request. Increment the Discarded Messages statistic.	Wait for Reply	23
Rx Valid Key Change	For OUTSTATION only. The outstation receives a correctly authenticated Key Change message.	Store new keys. Set Key Status = OK. Transmit Key Status message. Reset Max Error Messages Sent Reset Max Authentication Rekeys	Security Idle	Discard the previously pending Critical ASDU. Store new keys. Set Key Status = OK. Transmit Key Status message. Cancel the Reply Timer. Reset Max Reply Timeouts. Reset Max Error Messages Sent Reset Max Authentication Rekeys	Security Idle	24
Rx Invalid Key Change	For OUTSTATION only. The outstation receives an improperly authenticated Key Change message.	Set Key Status = AUTH_FAIL. Transmit Key Status message.	Security Idle	Discard the invalid Key Change message. Increment Unexpected Messages statistic Increment Discarded Messages statistic	Wait for Reply	25
Rx Challenge	The device receives a Challenge message.	Reply as described in 7.5.3 Responder procedures	Security Idle	Reply as described in 7.5.3 Responder procedures	Wait for Reply	26

Event	Event Description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard DNP3 protocol.		The device is waiting for the other device to authenticate itself.		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Authority Changes User Status	For MASTER only. The master receives from the authority some new Certification Data for a particular user.	IF the master and outstation support remotely changing Update Keys: Transmit the Certification Data in a new User Status Change message or User Certificate message as appropriate.. Start the Reply Timer.	Wait for User Change Response (Table 7-14)	Queue the event and process it after returning to Security Idle state.	Wait for Reply	27
Outstation Restarted	For MASTER only. The master receives a response or unsolicited response with the RESTART internal indication set when it was not set previously. If this occurs, execute this row rather than the row that would be normally executed. This would normally indicate that the outstation Session Keys need to be re-initialized. In case of an attack, the re-keying is throttled using the Rekeys Due to Restarts statistic.	IF Rekeys Due to Restarts <= Max Rekeys Due to Restarts Discard ASDU containing the RESTART indication Increment Discarded Messages statistic Increment Rekeys Due to Restarts statistic Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 7-13)	IF Rekeys Due to Restarts <= Max Rekeys Due to Restarts Discard the critical ASDU that was queued pending authentication. Discard ASDU containing the RESTART indication Increment the Discarded Messages statistic twice Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 7-13)	28
		IF Rekeys Due to Restarts > Max Rekeys Due to Restarts Discard ASDU with the RESTART indication Increment Discarded Messages statistic	Security Idle	IF Rekeys Due to Restarts > Max Rekeys Due to Restarts Discard ASDU with the RESTART indication Increment Discarded Messages statistic	Wait for Reply	29

7.5.2.4 Error Messages

As described more formally in Table 7-8, devices may initially respond to error conditions by transmitting Error messages. Error messages contain a code indicating the type of error, and optionally contain a UTF-8 text string encoded according to RFC 3629 describing the error in more detail for debugging purposes. To help protect against denial-of-service attacks, a device shall stop transmitting Error messages after it has counted a number of errors that exceeds a Max Error Messages Sent described in 7.6.1.4.2. Devices may also choose to not send error messages at any time, regardless of error count.

Note that error messages may be transmitted on a DNP association other than the one on which authentication is performed. This may be extremely useful for detecting attacks and is therefore recommended. It is also recommended that all errors be logged.

Table 7-9 illustrates how error messages are implemented in DNP3.

Table 7-9: Use of Error Message Objects in DNP3

Function Code	Object Variation	Behavior	Purpose
0x83 Authentication Response 0x21 Authentication Request – No Ack	g120v7 Authentication Error (as an Info object)	Response to a security message on the same DNP association	Notify other device of a possible configuration error or lack of synchronization
0x81 Response 0x82 Unsolicited Response	g120v7 Authentication Error (as an Event object)	Included with other DNP data in an event response on the other DNP association	Detection of an attack (see note below)

NOTE—When the Error Message is sent as an event using function codes 0x81 or 0x82, the CON bit shall be set. The rule regarding CON bits in Authentication Responses in 7.5.2.3.1 does not apply.

7.5.3 Responder procedures

7.5.3.1 Responder Role

A device, either master or outstation, that supplies authentication data shall be called a Responder. Each Responder shall follow the procedures described in this subclause.

7.5.3.2 Responding to Challenges

A Responder shall respond to a Challenge message with a correctly-formed Reply message within an acceptable Reply Timeout defined per system as described in 7.6.1.4.1.

If the following conditions are met:

- The Responder is a master
- The Authentication Challenge object is in a normal DNP3 response (function code 0x81 or 0x82)
- The CON bit is set in the response

Then, the master shall, instead of transmitting an Authentication Reply object, shall transmit a Confirm (0x00) message in aggressive mode, i.e. containing:

— Function Code 0x00 Confirm

— Authentication Aggressive Mode Request object (g120v3)

— Authentication MAC object (g120v9)

The rationale for this rule and an example are found in 7.5.2.3.2.

A Responder shall not proceed with further communications until it has successfully responded to the Challenge message. This rule includes not responding to any subsequent Challenge messages until the current Challenge is completed.

Upon responding to a Challenge, the Responder shall increment the Critical Messages Sent statistic, counting the original critical ASDU that was challenged.

7.5.3.3 Aggressive Mode

Aggressive mode, in which a device supplies authentication information in the same ASDU as the data it is authenticating, shall be implemented by all DNP3 devices conforming to this standard.

These devices shall also provide a mode of operation in which Aggressive Mode is disabled.

A Responder that uses Aggressive Mode shall place a correctly-formed Aggressive Mode Request within the ASDU being authenticated. A Responder shall not transmit an Aggressive Mode Request until it has successfully responded to at least one Challenge message each time the master changes the Session Keys. In other words, the Responder shall send the first critical ASDU after a Session Key change as a normal DNP3 message, not as an Aggressive Mode Request.

Upon transmitting an Aggressive Mode Request, the Responder shall increment the Critical Messages Sent statistic.

7.5.3.4 Authentication Errors

If the Responder receives an Error Message with reason <1> Authentication Failed after sending an Authentication Reply or Aggressive Mode Request object, the most likely reason is that the Session Keys used in the authentication have become invalid due to a timeout. This may indicate that the master's Session Key change interval or the outstation's expected Session Key change interval or the corresponding counts are incorrectly configured to be too small.

The other reason a Responder may receive an Error Message with reason <1> Authentication Failed is that an attacker may be trying to provoke the Responder into taking action resulting in a denial of service.

For these reasons, the following rules apply:

a) An outstation shall not automatically retry sending an Aggressive Mode Request in an Unsolicited Response if the master sends an Error message.

b) An outstation may retry sending an Aggressive Mode Request in an Unsolicited Response only due to an application layer timeout. Since application layer retries are not permitted in DNP3 except for Unsolicited Responses, this is the only case in which an authentication retry might occur.

c) If a user queues critical data for transmission by the master and the master is in Security Idle state, the master shall transmit the data even if the last Key Status it received from the outstation was not OK, i.e. the Session Keys are invalid and the master was waiting for the Session Key change interval before changing the keys. If the outstation then returns an Error message with reason <1> Authentication Failed, the master shall send a Key Status Request and enter the Wait for Key Status state, attempting to change the Session Keys. This shall only occur when the user queues critical data.

d) If the master receives an Error Message with reason <1> Authentication Failed, but it later succeeds in changing the Session Keys, it may optionally reduce the Session Key change interval and count, with the intent of preventing a subsequent failure. It may do so only once.

7.5.4 Master Procedures

7.5.4.1 Master Role

In addition to acting as a Challenger and a Responder, Masters shall follow the procedures described in this subclause in order to initialize and change user keys, status and roles at the outstation.

7.5.4.2 Changing Session Keys

There shall be two Session Keys, one used for authenticating data in the Monitoring Direction, and one for authenticating data transmitted in the Control Direction, as described in Table 7-1. The outstation and masters shall maintain a unique set of Session Keys for each user of the outstation, and a default set of Session Keys used for cases when the master acts for multiple users (as in the case of a poll, for instance), or when the outstation initiates the security message sequence.

Each master shall initialize the Session Keys upon establishing communications or when it detects the outstation has restarted, and periodically change the Session Keys as described in Table 7-13. The change interval shall be set using a configurable parameter as discussed in 7.6.1.4.3.

The master shall use a symmetric Update Key to encrypt the Session Keys and transmit them to the outstation in a Key Change message. An Update Key shall be separately assigned for each combination of user and outstation. Each master shall also act as a default user of the outstation under the conditions described in Table 7-11. There shall be a separately assigned Update Key and set of Session Keys for that default user on the outstation. It is possible for this default user to be the only user.

The master shall consider an attack to be underway if the MAC on a Session Key Status object is found to be invalid using the most recently valid Monitoring Direction Session Key.

7.5.4.3 Deriving Keys

All keys used in implementing this standard shall be derived in a pseudo-random manner that makes it difficult to predict what the next key will be. A variety of algorithms exist for deriving cryptographic keys and the appropriate algorithm may vary depending on the environment in which DNP3 is used. The key derivation algorithm chosen shall be an open standard, appropriate for the use being made of DNP3, consistent with the security policies of the organization implementing this standard and compliant with any regulatory requirements. Some recommended standards for key derivation are NIST SP 800-108 and ISO/IEC 18033-2. The Device Profile Document for each device shall specify the key derivation algorithm used.

7.5.4.4 Assigning User Numbers

The master and outstation shall identify with a unique User Number each set of Session Keys that they share. The master shall be responsible for initiating the assignment of User Numbers; the outstation shall be responsible for choosing the actual number for each user. Each security message contains the applicable User Number and therefore specifies the applicable set of Session Keys. The purpose of User Numbers is to make individual human beings accountable for the critical operations they perform remotely on the outstation.

Figure 7-29 shows an example of how User Numbers may be assigned. In this example, there are two masters, each of which has two users, communicating with a single outstation. When a user initiates a critical operation that sends DNP messages from a master to an outstation, the master is responsible for authenticating that operation using the appropriate User Number and corresponding Session Keys for that user.

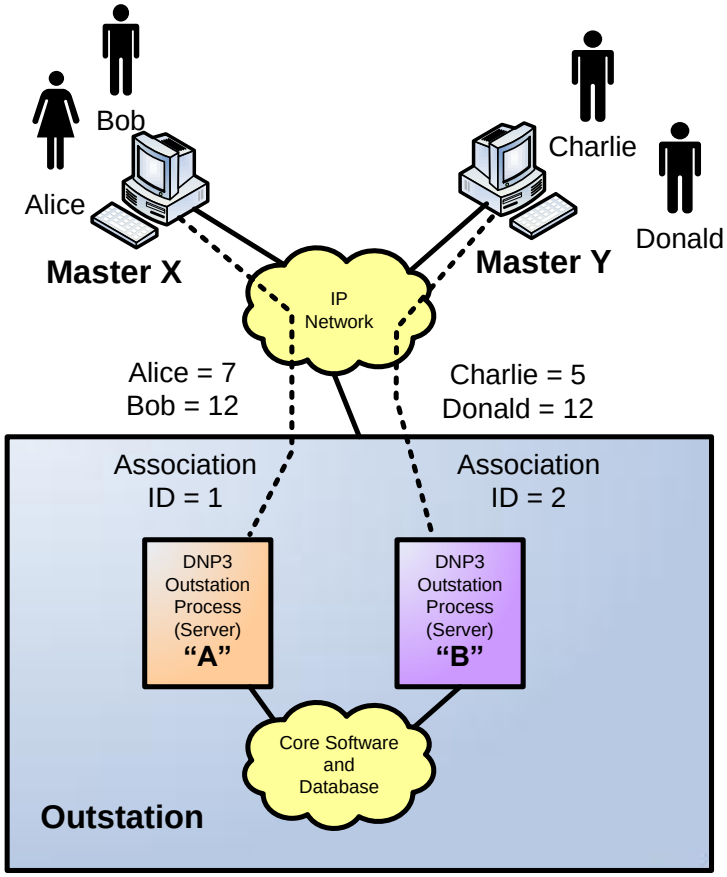


Figure 7-29: Example of User Number and Association ID Assignments

Note that in the example, both Bob and Donald have the same User Number. User Numbers need not be unique within the entire outstation, only within a particular DNP association. The precise definition of a DNP association is found in Annex C, but it essentially means the logical connection between a particular master and a particular outstation.

In the example, there are two associations, one from the single outstation to each master. The figure shows a separate software process for each association, but this is done purely for illustration; the associations may be implemented many different ways. Each association uses a particular set of addresses for the master and the outstation. The addresses may include DNP data link layer addresses, IP addresses, TCP or UDP port numbers, serial port numbers, and internal software identifiers.

Within a particular association, the User Number uniquely identifies a particular user. For most of the security messages, this is sufficient identification. However, there is one exception. As noted in 7.5.2.4, this standard recommends that Error messages be transmitted on associations other than that on which the error occurred, in order to help with intrusion detection.

Devices must therefore include in each Error message an Association ID, which is an integer uniquely identifying the DNP association and the complete set of addresses it uses. The combination of Association ID and User Number shall uniquely identify a user with an entire device. Table 7-10 shows that in the example, the Association IDs are simply the numbers "1" and "2".

Table 7-10: Example of User Number and Association ID Assignments

Association ID	User Number	User	Master	Outstation Process
1	0	Unknown	X	A
1	1	Default	X	A
1	7	Alice	X	A
1	12	Bob	X	A
2	0	Unknown	Y	B
2	1	Default	Y	B
2	5	Charlie	Y	B
2	12	Donald	Y	B

Note that in each association, the outstation uses the reserved User Number <0> when it is issuing a Challenge but does not yet know the user associated with the critical ASDU it is challenging. The outstation and master also use a second reserved User Number <1> as the default User Number in a number of different situations, as illustrated in Table 7-11.

Table 7-11: When to Use the Reserved User Numbers

Case	User Number
Outstation sends Challenge	Unknown <0>
Outstation sends Aggressive Mode unsolicited response	Default <1>
Outstation sends Aggressive Mode response	Default <1>
Master Challenges unsolicited response from outstation	Default <1>
Master Challenges response from outstation	Default <1>
Master sends common request (e.g. poll) for data to be processed by multiple users.	Default <1>
Any other case	<2…65535>

7.5.4.5 Changing User Status

A master or outstation may optionally permit remotely changing Update Keys using DNP3. There are two possible methods for changing Update Keys based on the type of cryptography used: symmetric, or asymmetric. Asymmetric cryptography is sometimes known as public key cryptography.

A master or outstation may implement one of the following options with respect to remotely changing Update Keys:

- Do not implement either method.
- Implement the symmetric method only.
- Implement both symmetric and asymmetric methods.

The process of changing Update Keys is based on the ISO/IEC 11770 standard (ISO/IEC 11770-2 and ISO/IEC 11770-3). Subclause 7.10 describes how it complies with this standard and summarizes the process using cryptographic notation.

The process of changing Update Keys begins with changing the status of a user. The status of a user includes the user's name, role, key and expiry interval, as described later in this subclause.

If the master and outstation both permit remotely changing Update Keys, the master shall promptly inform the outstation of changes made by an authority to the status of a user and to the user's Update Keys, as described in Table 7-14.

The authority shall *not* be the master station itself, but is otherwise not described by this standard. The communication between the authority and the master station shall be secured but is assumed to be a protocol suite other than DNP3. It is therefore not discussed in this standard. Similarly, the authentication of the actual user and the association of the user with the User Name and other information described below must be a secure process, but one that is out of the scope of this standard. 7.6.1.4.10 contains some notes on this topic.

The authority may add users, delete users or change the information associated with a user via the master station. The information associated with each user (known as the Certification Data) shall be specified in either the User Status Change (g120v10) object or the User Certificate (g120v8) object, and shall include:

- **User Name**. The name of the user shall be unique within the organization managed by the authority, with one exception: the null-terminated UTF-8 string "Common" shall be used to identify the default Update Key, User Number <1> used between the master and the outstation. The format of the User Name is otherwise outside the scope of this standard.
- **User Role**. The authority may change the Role of the user. The Role of the user shall determine what actions a user is allowed to perform on the outstation, as described in Table 7-12. These roles are defined in IEC 62351-8. No user is permitted to change the Role of another user; only the authority may do so.
- **User Public Key** (optional). The authority may change the Update Key for the user. The master shall provide the new Update Key to the outstation in a confidential, authenticated manner as described in Table 7-14. If the Update Key Change Method is asymmetric, the master shall supply the user's Public Key to the outstation, un-encrypted but digitally signed by the authority using the Authority Private Key, in the User Status Change (g120v10) object, and shall supply the new Update Key later in the process.
- **Expiry Interval**. The authority may change the time when the Role of the user and the validity of the Update Key will expire.

Table 7-12: User Roles

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 ..32767>	RESERVED	For future use.						
<32768 ..65535>	PRIVATE	Defined by external agreement. Not guaranteed to be interoperable.						

The authority, master, and outstation may use either symmetric or asymmetric cryptography to change the status, Role, Expiry Interval, or Update Key of a user. The method used, including the set of cryptographic algorithms and

DNP3 objects, shall be preconfigured at the master as described in 7.6.1.4.9 and the master shall specify it to the outstation in the User Status Change (g120v10) object or the User Certificate (g120v8) object. The certificate shall conform to the X.509 format as described in IETF RFC 5280, RFC 5755, and IEC 62351-8.

The key used to produce the Certification Data shall not be known to the master. If it is symmetric, it shall be known only to the authority and the outstation. If it is asymmetric, it shall be a private key known only to the authority, with the corresponding public key known to the outstation.

If the authority changes the Role or Expiry Interval of a user, the authority shall also change the Update Key of that user.

The authority shall not re-use Update Keys for the same user over the lifetime of the system.

The authority shall provide the master with Certification Data for the default user before the master begins communicating with the outstation. If the outstation is not pre-configured with the default user, the master shall add that user before beginning secure communications with the outstation.

7.5.4.6 Changing Update Keys

If the master and outstation both permit remotely changing Update Keys, the master may change the Update Key of a user at any time after it has forwarded the Certification Data to the user in a User Status Change (g120v10) or User Certficate (g120v8) object. The master shall do so by sending an Update Key Change Request (g120v11) object containing the User Name of the user and some random challenge data. It is recommended that the master begin the Update Key Change process soon after the status change, since any changes to Role or Expiry Interval shall not take effect until the master completes this process.

Upon receiving an Update Key Change Reply (g120v12) object from the outstation, the master shall obtain the Encrypted Update Key Data to send to the outstation in an Update Key Change object (g120v13). As described in the definition of that object, the Encrypted Update Key Data shall consist of the following data, encrypted together:

- The name of the user
- The random challenge data sent from outstation in the Update Key Change Reply
- The new Update Key for the user

The master shall take different actions to obtain the Encrypted Update Key Data and to authenticate the transfer of this data depending on the Update Key Change Method in use:

- If the Update Key Change Method is **symmetric**, the master shall obtain the Encrypted Update Key Data from the authority. The method used to do so is outside the scope of this standard but the communication must be secured. The authority shall encrypt the Update Key Data using the symmetric key it shares with the outstation (i.e. the Authority Certification Key described in Table 7-1). The master shall authenticate the transfer of the Encrypted Update Key Data by sending an Update Key Change Confirmation (g120v15) object with the Update Key Change (g120v13) object in its request. In this way, the master authenticates the transfer of the Encrypted Update Key Data using the new Update Key itself.
- If the Update Key Change Method is **asymmetric**, the master shall create the Encrypted Update Key Data using the outstation's Public Key. The master shall authenticate the transfer of the Encrypted Update Key Data by sending an Update Key Change Signature object (g120v14) with the Update Key Change (g120v13) object in its request. In this way, the master authenticates the transfer of the Encrypted Update Key Data by signing it with the User's Private Key. The authority securely provided the outstation with the User's Public Key in the User Status Change (g120v10) object, so the outstation can verify that the master is authentic and the master and authority agree on the new Update Key.

— Using either method, if the master does not wish to actually change the Update Key, it can instead authenticate itself to the outstation and verify that the outstation has the correct Update Key by sending only an Update Key Change Confirmation (g120v15) object, which will cause the outstation to reply with an Update Key Change Confirmation.

Upon receiving an Update Key Change Confirmation (g120v15) object from the outstation, the master shall verify that the Message Authentication Code (MAC) in that object is valid. , The master calculates this MAC using the random challenge data from both itself and the outstation, the user's name, the User Number (USR) and the Key Change Sequence Number (KSQ). If the MAC is valid, the master shall begin using the new Update Key and User Number for Session Key changes.

If the Update Key change process fails at any point, as discussed in Table 7-14 the master shall inform a human of the failure and shall continue to use the previous Update Key for Session Key changes. It is expected that the process will be re-initiated by a human rather than being automatically re-initiated. However, that is beyond the scope of this standard.

7.5.4.7 Master State Machine

The master shall execute the state machine described in Table 7-13 and Table 7-14.

Table 7-13: Master State Machine – Changing Session Keys

Event	Event Description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The master is waiting for the outstation to send any Key Status message.		The master is waiting for the outstation to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Init	The master has initialized	Transmit a Key Status Request message. Start the Reply Timer.	Wait for Key Status	Not possible.	Not possible.	1
Rx Key Status <> OK	The master receives a Key Status message with the Key Status set to a value other than <1> OK.	Transmit a Key Change message. Start the Reply Timer.	Wait for Key Change Confirmation	Increment Unexpected Messages statistic.	Wait for Key Change Confirmation	2
Rx Key Status = OK	The master receives an authentic Key Status message with the Key Status set to <1> OK.	Transmit a Key Change message. Start the Reply Timer.	Wait for Key Change Confirmation	Start the Key Change timer and reset the Key Change counter. Reset Max Authentication Failures. Reset Max Authentication Rekeys	Security Idle	3
Reply Timeout	The Reply Timer has expired while the master was waiting for a response from the outstation.	Increment Reply Timeouts statistic. Transmit a Key Status Request message. Start the Reply Timer.	Wait for Key Status	Increment Reply Timeouts statistic. Transmit a Key Status Request message. Start the Reply Timer.	Wait for Key Status	4
Max Reply Timeouts Exceeded	• The Reply Timeouts statistic has exceeded Max Reply Timeouts • The protocol has detected a communications failure for some other reason. This event affects all users. Refer to 7.6.1.4.1 for details regarding the Reply Timer.	Increment Failed Session Key Changes statistic. Start the Key Change timer and reset the Key Change counter.	Security Idle	Increment Failed Session Key Changes statistic. Start the Key Change timer and reset the Key Change counter.	Security Idle	5

Event	Event Description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The master is waiting for the outstation to send any Key Status message.		The master is waiting for the outstation to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Key Change Timeout	Either the Key Change Timer has expired on the master, or the number of transmitted or received protocol messages has exceeded the Message Count Threshold. This event should not happen in either of these states for the current user.	IF the timer is for the same user, discard. IF the timer is for a different user, queue the event and process it when next in Security Idle state.	Wait for Key Status	IF the timer is for the same user, discard. IF the timer is for a different user, queue the event and process it when next in Security Idle state.	Wait for Key Change Confirmation	6
Rx Challenge message	The master receives a Challenge message or Aggressive Mode Request message even though the Session Keys are not yet valid.	Increment Unexpected Messages statistic. Increment Authentication Failures statistic. Discard the Challenge message. Increment Discarded Messages statistic.	Wait for Key Status	Increment Unexpected Messages statistic. Increment Authentication Failures statistic. Discard the Challenge message. Increment Discarded Messages statistic.	Wait for Key Change Confirmation	7
Rx Critical ASDU	The master receives an ASDU that requires authentication even though the Session Keys are not yet valid.	Increment Unexpected Messages statistic. Increment Authentication Failures statistic. Discard the Critical ASDU. Increment Discarded Messages statistic.	Wait for Key Status	Increment Unexpected Messages statistic. Increment Authentication Failures statistic. Discard the Critical ASDU. Increment Discarded Messages statistic.	Wait for Key Change Confirmation	8
Rx Unsolicited Non-Critical ASDU	The master receives an ASDU that does not require authentication and was spontaneously transmitted by the outstation.	Process the ASDU and issue a Confirm if required.	Wait for Key Status	Process the ASDU and issue a Confirm if required.	Wait for Key Change Confirmation	9

Event	Event Description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The master is waiting for the outstation to send any Key Status message.		The master is waiting for the outstation to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Inappropriate Non-Critical ASDU	The master receives a non-critical, non-authentication ASDU in response to its previous authentication message, or receives some other indication that the outstation may not be capable of processing authentication messages.	Increment Unexpected Messages statistic. Increment Failed Session Key Changes statistic. Process the ASDU and issue a Confirm if required. Start the Key Change Timer and reset the Key Change Counter.	Security Idle	Increment Unexpected Messages statistic. Increment Failed Session Key Changes statistic. Process the ASDU and issue a Confirm if required. Start the Key Change Timer and reset the Key Change Counter.	Security Idle	10
A User Wants to Transmit an ASDU	A user wishes to transmit from this master. May be either a critical or non-critical ASDU.	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Key Status	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Key Change Confirmation	11
Rx Unexpected Key Status	The master receives a Key Status message for a user other than the one which is currently in Wait for Key Status or Wait for Key Change Confirmation state. This event should not occur because the outstation should be responding to a request for THIS user	Increment Unexpected Messages statistic. Discard the Key Status message. Increment Discarded Messages statistic.	Wait for Key Status	Increment Unexpected Messages statistic. If the Key Status message was not authentic, Increment Authentication Failures statistic. Discard the Key Status message. Increment Discarded Messages statistic.	Wait for Key Status	12

Event	Event Description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The master is waiting for the outstation to send any Key Status message.		The master is waiting for the outstation to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Invalid Key Status	Receives a Key Status = OK, but the message is not authentic.	Increment Authentication Failures statistic. Discard the Key Status message. Increment Discarded Messages statistic.	Wait for Key Status	As in Rx Unexpected Key Status, above	Wait for Key Status	13
Rx Initial Key Status	Receives a Key Status = OK, but the Master has just restarted, so the session keys are not yet valid and the Master cannot authenticate the message.	Transmit a Key Change message. Start the Reply Timer.	Wait for Key Change Confirmation	As in Rx Unexpected Key Status, above	Wait for Key Status	14
Max Authentication Failures	As a result any of the other events, the Max Authentication Failures for this user was exceeded. The master has unsuccessfully tried several times to reset the Session Keys for this user. Must give another user a chance to initialize keys.	Start the Key Change Timer. Reset the Key Change Counter. Increment Failed Session Key Changes statistic.	Security Idle	Start the Key Change Timer. Reset the Key Change Counter. Increment Failed Session Key Changes statistic.	Security Idle	15

Table 7-14: Master State Machine – Changing Update Keys

Event		State						
		Wait for User Change Response		**Wait for Update Key Reply**		**Wait for Update Key Confirmation**		
		The master is waiting for the outstation to send a response to a User Status Change request.		The master is waiting for the outstation to reply to an Update Key Change request.		The master is waiting for the outstation to send an Update Key Confirmation response.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	B	C	**D**	**E**	**F**	**G**	**H**	
Rx Null Response (with no IINs set)	None	IF the User Status Change must be applied immediately, Transmit Update Key Change Request (g120v11). Restart the Reply Timer. Reset Max Reply Timeouts.	Wait for Update Key Reply	Log the event. Increment the Unexpected Messages statistic.	Wait for Update Key Reply	Log the event. Increment the Unexpected Messages statistic.	Wait for Update Key Confirmation	1
		IF the User Status Change need not be applied immediately, take no further action.	Security Idle					
Rx Update Key Change Reply	g120v12	Discard the Reply. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for User Change Response	Transmit Signed Update Key Change (g120v13) and either Update Key Change Signature (g120v14) or Update Key Change Confirmation (g120v15). OR Transmit only an Update Key Change Confirmation (g120v15). Restart the Reply Timer. Reset Max Reply Timeouts.	Wait for Update Key Confirmation	Transmit Signed Update Key Change (g120v13) and either Update Key Change Signature (g120v14) or Update Key Change Confirmation (g120v15). OR Transmit only an Update Key Change Confirmation (g120v15). Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Confirm-ation	2

Event		State						
		Wait for User Change Response		**Wait for Update Key Reply**		**Wait for Update Key Confirmation**		
		The master is waiting for the outstation to send a response to a User Status Change request.		The master is waiting for the outstation to reply to an Update Key Change request.		The master is waiting for the outstation to send an Update Key Confirmation response.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	B	C	**D**	**E**	**F**	**G**	**H**	
Rx Valid Update Key Change Confirmation	g120v15	Discard the Confirmation. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for User Change Response	Discard the Confirmation. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for Update Key Reply	Increment the Successful Authentications statistic. Increment the Update Key Changes statistic IF the key was changed. Cancel the Reply Timer. Begin using the new Update Key for subsequent authentications.	Security Idle	3
Rx Invalid Update Key Change Confirmation	g120v15	Discard the Confirmation. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for User Change Response	Discard the Confirmation. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for Update Key Reply	Discard the Confirmation. Increment the Discarded Messages statistic. Increment the Authentication Failed statistic. Increment the Failed Update Key Changes statistic. Cancel the Reply Timer. IF Error Messages Sent <= Max Error Messages Sent Transmit Error (g120v7). Increment Error Messages Sent. Log the event.	Security Idle	4

Event		State						
		Wait for User Change Response		**Wait for Update Key Reply**		**Wait for Update Key Confirmation**		
		The master is waiting for the outstation to send a response to a User Status Change request.		The master is waiting for the outstation to reply to an Update Key Change request.		The master is waiting for the outstation to send an Update Key Confirmation response.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	B	C	**D**	**E**	**F**	**G**	**H**	
Reply Timeout	None	Transmit User Status Change (g120v10). Restart the Reply Timer. Increment Reply Timeouts Statistic	Wait for User Change Response	Transmit Update Key Change Request (g120v11). Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Reply	Transmit Update Key Change (g120v13) and either Update Key Change Signature (g120v14) or Update Key Change Confirmation (g120v15). OR Transmit only an Update Key Change Confirmation (g120v15). Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Confirm-ation	5
MaxReply Timeouts Exceeded	None	Increment Failed Update Key Changes statistic	Security Idle	Increment Failed Update Key Changes statistic	Security Idle	Increment Failed Update Key Changes statistic	Security Idle	6
Rx Error Internal Indication	None	Increment Failed Update Key Changes statistic Log the event. Cancel the Reply Timer.	Security Idle	Increment Unexpected Messages statistic Log the event.	Wait for Update Key Reply	Increment Unexpected Messages statistic Log the event.	Wait for Update Key Confirm-ation	7
Rx Error	g120v7	Increment Failed Update Key Changes statistic Log the event. Cancel the Reply Timer.	Security Idle	Increment Failed Update Key Changes statistic Log the event. Cancel the Reply Timer.	Security Idle	Increment Failed Update Key Changes statistic Log the event. Cancel the Reply Timer.	Security Idle	8
Rx Critical ASDU	Varies	Queue the ASDU until the next time the master enters Security Idle state.	Wait for User Change Response	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Update Key Reply	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Update Key Confirm-ation	9

Event		State						
		Wait for User Change Response		**Wait for Update Key Reply**		**Wait for Update Key Confirmation**		
		The master is waiting for the outstation to send a response to a User Status Change request.		The master is waiting for the outstation to reply to an Update Key Change request.		The master is waiting for the outstation to send an Update Key Confirmation response.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	B	C	**D**	**E**	**F**	**G**	**H**	
A User Wants to Transmit an ASDU	Varies	Queue the ASDU until the next time the master enters Security Idle state.	Wait for User Change Response	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Update Key Reply	Queue the ASDU until the next time the master enters Security Idle state.	Wait for Update Key Confirm-ation	10
Rx Unsolicited Non-Critical ASDU	Varies	Process the ASDU and issue a Confirm if required.	Wait for User Change Response	Process the ASDU and issue a Confirm if required.	Wait for Update Key Reply	Process the ASDU and issue a Confirm if required.	Wait for Update Key Confirmation	11
Rx Inappropriate Non-Critical ASDU	Varies	Increment Unexpected Messages statistic Increment Discarded Messages statistic Discard the non-critical ASDU Log the event.	Wait for User Change Response	Increment Unexpected Messages statistic Increment Discarded Messages statistic Discard the non-critical ASDU Log the event.	Wait for Update Key Reply	Increment Unexpected Messages statistic Increment Discarded Messages statistic Discard the non-critical ASDU Log the event.	Wait for Update Key Confirm-ation	12

7.5.5 **Outstation procedures**

7.5.5.1 Outstation Role

In addition to acting as a Challenger and a Responder, each outstation shall follow the procedures described in this subclause, permitting the Master to initialize and change Session Keys and to change the status, Role, Expiry Interval and Update Keys of users.

7.5.5.2 Key Status

The outstation shall maintain an internal variable having the possible values of Key Status described in the definition of the Authentication Key Status object, and return this value in response to each Key Status Request Message.

The outstation shall set the Key Status to <1> NOT_INIT upon startup of the outstation.

If the number of Key Status Requests received by the outstation exceeds a configured threshold within the Expected Session Key Timeout, the outstation shall notify a human as described in 7.6.1.4.6.

The outstation shall calculate pseudo-random Challenge Data according to FIPS 186-2 and include it in the Key Status message.

7.5.5.3 Authenticating Session Key Changes

Upon receiving a Key Change message, the outstation shall unwrap the Key Wrap Data in the Key Change message using the current Update Key.

If the Key Status information in the Key Wrap Data matches the last Key Status information transmitted by the outstation, the outstation shall consider the Key Change message authentic and valid.

If any of the unwrapped Key Status information does not match the last Key Status information transmitted by the outstation, the outstation shall consider the Key Change message invalid.

7.5.5.4 Changing Session Keys

The outstation shall respond to a Key Change message within an acceptable Reply Timeout defined per system as described in 7.6.1.4.1.

The outstation shall be configured with a timer such that it shall invalidate a set of Session Keys if it has not received a Key Change message within that interval as described in 7.6.1.4.5

7.5.5.5 Changing User Status

Upon receiving a User Status Change (g120v10) objec t or a User Certifcate (g120v8) object, the outstation shall validate the Certification Data (including User Name, Role, Expiry Interval and new Update Key or public key for the user) in that object as follows:

- Verify that the outstation supports the specified Update Key Change Method (see 7.6.1.4.9).
- Verify that the Certification Data was created by the authority, using the authority's credentials that were pre-configured at the outstation:
    1) If the Update Key Change Method is **symmetric**, validate the MAC of the Certification Data using the symmetric key shared between the outstation and the authority (the Authority Certification Key).
    2) If the Update Key Change Method is **asymmetric**, validate the authority's digital signature against the Authority Public Key.

— Verify that the Status Change Sequence Number is larger than any previously received for this user.

— If a User Certificate was supplied, verify the Area of Responsibility text string in the certificate matches at least one such string preconfigured for this outstation.

If the User Status Change or User Certificate is invalid (and the Maximum Error Count has not been exceeded), the outstation shall transmit an Error message (g120v7) with the error <8> Update Key Change Method Not Permitted, or <9> Invalid Signature, or <10> Invalid Certification Data.

If the User Status Change is valid, the outstation shall store the Certification Data for later use.

If the authority deletes a user, the outstation shall invalidate all keys associated with that user immediately.

If the authority adds a user or changes the Role or Expiry Interval of a user, the outstation shall not apply the changes until the Update Key has been successfully changed, including mutual authentication of the master and outstation.

When the Update Key has been successfully changed, the outstation shall calculate the new Expiry Interval of the User Role based on the last User Status Change object it received. The Expiry Interval shall be the specified number of days from the reception of the User Status Change object, to the nearest second. The outstation shall ensure that the Expiry Interval is correct relative to the reception of the User Status Change regardless of what time is set at the outstation or how many times it is changed.

NOTE—If the authority changes the Role or Expiry Interval of a user, the authority shall also change the Update Key of that user.

7.5.5.6 Changing Update Keys

Upon receiving a Key Change Request (g120v11) object, the outstation shall verify that the specified User Name was previously validated and stored at the outstation, and the Expiry Interval of the User has not been exceeded.

If the User Name is non-existent or expired, the outstation shall respond with an Authentication Error (g120v7) object having the reason <11> Unknown User.

If the User Name is valid, the outstation shall respond with an Update Key Change Reply (g120v12) object containing a new Key Change Sequence Number, a User Number to be used to identify the user, and random challenge data calculated according to FIPS 186-2.

The next step of the Update Key change process, the reception and authentication of the Update Key Change, shall differ depending on the method used:

— If the Update Key Change Method used by the outstation is **symmetric**, upon receiving an Update Key Change (g120v13) object from the master, the outstation shall validate the accompanying Update Key Change Confirmation (g120v15). If the Message Authentication Code is valid, the outstation shall begin using the new Update Key for session key changes.

— If the Update Key Change Method used by the outstation is **asymmetric**, upon receiving a Update Key Change (g120v13) object from the master, the outstation shall validate the digital signature of the user with the User Public Key previously certified by the authority. If the signature is correct, the outstation shall begin using the new Update Key for session key changes.

— Using either method, upon receiving an Update Key Change Confirmation (g120v15) without an Update Key Change (g120v13) object, the outstation shall validate the Update Key Change Confirmation object. If the Message Authentication Code is valid, the outstation may proceed with the next step.

If the Update Key Change or the Update Key Change Confirmation was correctly authenticated, the outstation shall send a response containing an Update Key Change Confirmation (g120v15) object. If it was not correctly authenticated and the Max Error Messages Sent has not been exceeded, the outstation shall respond with an Error (g120v7) object with error code <1> Authentication Failed.

7.5.5.7 Enforcing User Roles

An outstation shall enforce the user Roles assigned by the authority as described in Table 7-12. The outstation shall not permit users to perform actions they do not have permission to perform, as designated by their Role, regardless of whether the user is authentic. The outstation shall reject such non-permitted actions by sending an Error (g120v7) object with the value <5> Authorization Failed.

If the authority deletes a user or if the Role of the user expires, an outstation shall invalidate the Update Key and any active Session Keys or Public Keys associated with the user. The outstation shall not make the expiry of the Update Key dependent on the time and date at the outstation. This standard assumes there is a reliable interval timer available at the outstation that is separate from the time and date. Ideally, this interval timer would continue even while the device was powered down, but this is not required. Upon startup, the outstation shall assume that only the default Update Key is valid until there is a trusted time source at the outstation (either through the protocol or some other source) with which to validate the Expiry Interval.

7.6 Interoperability Requirements

This subclause describes which capabilities shall be considered to fall into the following categories:

- Mandatory to ensure interoperability between devices
- Optional but required to be tested if implemented
- Recommended practices

7.6.1 Minimum Requirements

This subclause describes the mandatory minimum capabilities required for a device to comply with this standard.

7.6.1.1 MAC Algorithms

Each device shall implement the MAC algorithms listed in this subclause.

7.6.1.1.1 HMAC-SHA-1

Each device shall permit the use of HMAC-SHA-1, as described in IEFT RFC 2104, IETF RFC 3174, and FIPS 186-2 to calculate the MAC Value. The MAC Value shall be the 160 bits (20 octets) output of the HMAC algorithm, truncated to either the leftmost 8 octets or the leftmost 10 octets. If this standard is used over TCP/IP, the truncated value shall be 10 octets. If it is used over serial links, the truncated value can be 8 octets. However, the longest practical MAC should be used whenever possible.

This is a mandatory MAC algorithm intended for use by devices with limited processing power that cannot otherwise implement DNP3 Secure Authentication with acceptable performance. All masters and outstations shall implement this algorithm for compatibility with such limited performance devices. However, this is not the preferred MAC algorithm. All devices shall provide a means to enable or disable the use of HMAC-SHA-1 by configuration.

7.6.1.1.2 HMAC-SHA-256

Each device shall permit the use of HMAC-SHA-256, as described in FIPS 180-2, to calculate the MAC Value. The MAC Value shall be the 256 bits (32 octets) output of the HMAC algorithm, truncated to either

the leftmost 8 octets or the leftmost 16 octets. When this authentication mechanism is used over TCP/IP, the truncated value shall be 16 octets. On serial implementations, it can be 8 octets. However, the longest practical MAC should be used whenever possible.

This shall be the default MAC algorithm.

7.6.1.2 Key Wrap / Transport Algorithms

Each device shall implement key wrap algorithms or key transport schemes as described in this subclause.

7.6.1.2.1 AES-128 Key Wrap

Each device shall permit the use of the Advanced Encryption Standard Key Wrap mechanism, as described in IETF RFC 3394, to encrypt and decrypt Session Keys or Update Keys. The Key Encryption Key (KEK) referred to in the Key Wrap specification shall be the Update Key. The default initialization vector shall be used.

7.6.1.3 Fixed values

Each device shall fix the following parameters to comply with this standard:

7.6.1.3.1 Minimum session key size

The minimum size of the Session Keys used to calculate the MAC Value shall be 128 bits.

7.6.1.3.2 Minimum update key size

The minimum size of the Update Key used to encrypt and decrypt Session Keys shall be 128 bits.

7.6.1.4 Configurable values

Each device shall permit changes to the parameters described in this subclause. Changes to these parameters shall be permanently retained over restarts of the device.

7.6.1.4.1 Reply timeout

The reply timeout used by devices to detect communication failures shall be settable in hundreds of milliseconds. The default value shall be 2 seconds. The maximum value shall be no less than 120 seconds.

7.6.1.4.2 Security Statistic Event Thresholds

Each device shall permit an event threshold to be configured for each of the security statistics listed in Table 7-6 in 7.5.2.2. If the statistic has incremented by the amount of the threshold since either startup or since the last time the statistic was reported as an event object (g122), the device shall generate an event object for that statistic.

The maximum value of each threshold shall be 65535. The default value of each threshold is listed in Table 7-6.

Note that when some of these thresholds are reached, the event shall cause the outstation to take specific actions—other than just reporting the change—as described in 7.5.2.2 and the state tables. The value of the statistic at which the threshold will next be reached is referred to by a particular name in the state tables. This maximum value is reset to its current value plus the configured value of the threshold each time the event occurs. These special statistics and the name of the corresponding maximum values are given in Table 7-15.

Table 7-15: Special Statistic Event Thresholds

Statistic	Name of Maximum Value (at which the statistic will next reach the threshold)
Authentication Failures	Max Authentication Failures
Reply Timeouts	Max Reply Timeouts
Rekeys Due to Authentication Failure	Max Authentication Rekeys
Error Messages Sent	Max Error Messages Sent
Rekeys Due to Restarts	Max Rekeys Due to Restarts

7.6.1.4.3 Session Key change interval

The session key change timeout used by the master to determine when to change session keys shall be settable in seconds up to 2 hours. The default value shall be 15 minutes. To accommodate systems which communicate infrequently (for instance every few hours or days), it shall be possible to disable the Session Key change interval and use only the Session Key change count. Alternately, the device may permit Session Key change intervals measured up to 1 week in length.

IMPORTANT NOTES:

a) Implementers should not increase the Session Key change interval beyond 30 minutes unless they also increase the size of the MAC Value. FIPS 198 requires MAC output to be truncated to no less than half its standard size, "unless an application or protocol makes numerous trials impractical". In the case of this authentication mechanism, the requirement for frequent changes of Session Keys fulfills this criterion and makes it possible to use shorter MAC Values.

b) An attacker could try to change Session Keys extremely frequently in order to deny service to legitimate users. It is recommended that DNP outstations implement a "watchdog" function over the Update Key Change and Failed Update Key Change statistics to prevent excessive Session Key changes. The details of such a mechanism are not discussed here.

c) An attacker could try to force a master to change Session Keys frequently by repeatedly sending Key Status objects with Status <> OK. As described in Table 7-13, the master shall not send Session Key Change messages any faster based on the Key Status it receives.

d) A master may optionally decrease the Session Key change interval if authentication failures are occurring, in case the failures are due to an incorrectly configured Expected Session Key change interval at the outstation. It may do so only once.

e) If the AES-GMAC algorithm is used, the Session Keys and Update Keys shall be changed frequently enough that AES-GMAC is used no more than 2^{21} times with the same key.

7.6.1.4.4 Session Key change count

The master shall also change session keys whenever a configured number of authentication ASDUs has been transmitted in either direction since the last key change. The value shall be settable from one in increments of one. The default value shall be 1000. The maximum value shall be no less than 10 000 and no more than half the maximum value of the Key Change Sequence Number (CSQ).

7.6.1.4.5 Expected Session Key change interval and message count

The outstation shall maintain a timer and a count between successive Key Change messages in the same manner as the master. The outstation shall invalidate the current set of Session Keys if they have not been changed within the configured interval. This rule will cause the Session Keys to become invalid whenever either the master or outstation times out, whichever happens sooner. To avoid excessive message exchanges it is recommended that the outstation interval and count be configured for twice the interval and count configured at the master.

7.6.1.4.6 Maximum Session Key Status Count

If the number of Session Key Status Requests received by the outstation exceeds this value within the Expected Session Key Change Interval, the outstation shall alert a human. If a different DNP association is in use, the outstation shall send an Error (g120v7) event object on that association with the code <12> Max Session Key Status Requests Exceeded. This value shall be configurable up to a maximum of 255 or down to 2. The default value shall be 5. This default means five session key changes were attempted within the time that one was expected. This count shall be kept per user of the outstation.

7.6.1.4.7 Use of aggressive mode

Aggressive Mode is considered optional by IEC 62351-5. However, it is not optional for DNP3. All DNP3 implementations claiming conformance to this standard shall implement it. They shall also permit it to be configured as disabled. If an outstation requests aggressive mode authentication of a Confirm (0x00) message as described in 7.5.2.3.2, the master shall do so regardless of whether aggressive mode is disabled.

7.6.1.4.8 Disabling authentication

Each device that supports this authentication mechanism shall permit this mechanism to be completely disabled by configuration on a per-association basis. It shall not be possible to change this configuration parameter remotely. The authentication mechanism shall be enabled by default.

7.6.1.4.9 Update Key Change Method

The method used for changing Update Keys shall be pre-configured at the master and specified to the outstation when the authority changes the status of a user. Each key change method specifies a particular set of cryptographic algorithms and DNP3 objects that shall be used. Only one method shall be active between a particular master and outstation.

Table 7-16 lists the possible values of Key Change Method. Numbers less than 64 represent the use of symmetric keys and algorithms, while numbers 64 through 127 represent the use of mostly asymmetric (public) keys and algorithms.

Devices are permitted to not implement remote changing of Update Keys, user status and Roles. If the master or outstation does not implement this feature and an Update Key is compromised, the Update Key must be changed via a mechanism outside the protocol.

All devices that permit remote changing of Update Keys shall implement Key Change Method <3>, the symmetric method employing AES-128 Key Wrap for encrypting keys and SHA-1-HMAC for authentication. This method is provided for use by devices with performance limitations. All devices shall permit this method to be disabled by configuration.

All devices that permit remote changing of Update Keys shall also implement Key Change Method <4>, the symmetric method employing AES-256 Key Wrap for encrypting keys and HMAC-SHA-256 for authentication. This method shall be the default.

All other Update Key Change Methods shall be optional. If a device implements Key Change Method <67>, the asymmetric method using HMAC-SHA-1, it shall permit this method to be disabled by configuration.

If asymmetric RSA algorithms are used for key transport, then the RSAES-OAEP algorithm shall be used for key transport as described in 7.6.2.2.2.

Table 7-16: Algorithms and Objects used for each Update Key Change Method

Key Change Method	Key Transport		Authentication and Integrity of User Credentials		Authentication of Master to Outstation and Outstation to Master		**Update Key Length (bits)**
	Algorithm	Objects	Algorithm	Objects	Algorithm	Object	
<0>	Not used						
<1>	Obsolete. Do not use.						
<2>	Obsolete. Do not use.						
<3>	AES-128 Key Wrap	g120v13	SHA-1-HMAC	g120v10	SHA-1-HMAC	g120v15	128
<4>	AES-256 Key Wrap	g120v13	SHA-256-HMAC	g120v10	SHA-256-HMAC	g120v15	256
<5>	AES-256 Key Wrap	g120v13	AES-GMAC	g120v10	AES-GMAC	g120v15	256
<3..63>	Reserved for future symmetric methods						
<64>	Obsolete. Do not use.						
<65>	Obsolete. Do not use.						
<66>	Obsolete. Do not use.						
<67>	RSAES-OAEP-1024 / SHA-1	g120v13	DSA SHA-1 (L=1024 N=160)	g120v10, g120v14	SHA-1-HMAC	g120v15	128
<68>	RSAES-OAEP-2048 / SHA-256	g120v13	DSA SHA-256 (L=2048 N=256)	g120v10, g120v14	SHA-256-HMAC	g120v15	256
<69>	RSAES-OAEP-3072 / SHA-256	g120v13	DSA SHA-256 (L=3072 N=256)	g120v10, g120v14	SHA-256-HMAC	g120v15	256
<70>	RSAES-OAEP-2048 / SHA-256	g120v13	DSA SHA-256 (L=2048 N=256)	g120v10, g120v14	AES-GMAC	g120v15	256
<71>	RSAES-OAEP-3072 / SHA-256	g120v13	DSA SHA-256 (L=3072 N=256)	g120v10, g120v14	AES-GMAC	g120v15	256
<72..127>	Reserved for future asymmetric methods						
<128..256>	Reserved for vendor-specific choices. Not guaranteed to be interoperable.						

The pseudo-random Challenge Data chosen by the master and outstation for changing Update Keys shall be as shown in Table 7-17 calculated according to FIPS 186-2.

Table 7-17: Size of Challenge Data

Authentication Algorithm	Size of Challenge Data
SHA-1-HMAC	160 bits, 20 octets
SHA-256-HMAC or AES-GMAC	256 bits, 32 octets

7.6.1.4.10 Cryptographic Information

Although this standard permits changing cryptographic keys remotely, each device must always have some information pre-configured. The type and number of keys and other cryptographic information that must be configured varies depending on the chosen Update Key Change Method, as shown in Table 7-18.

Devices shall retain all the information listed in Table 7-18 and the correspondence between these pieces of information over restarts, except the Session Keys. They are reinitialized after each restart.

NOTES for Table 7-18:

1) Using the asymmetric method, it is possible for the Update Key to be derived by the master and not known to the authority at all. This is not possible using the symmetric method.

2) It is not necessary for the master to know the authority's public key for any DNP3 transaction. However, the master may need the authority's public key for other reasons unrelated to this standard.

3) The master must know the user's private key in order to sign the Update Key for the outstation. The authority must know the user's public key to certify it to the outstation. One solution for achieving these requirements may be for the authority to derive both keys and encode them on a token for the user to carry and insert at the master. Another may be for the master to derive both keys and securely provide the user's public key to the authority for certification. There may be other solutions. The solution chosen is out of the scope of this standard. The master always receives the user's public key in certification by the authority, even if it was originally derived by the master.

4) If the Update Key is not to be changed remotely, the Update Key and the corresponding User Number (USR) must be pre-configured at the outstation. The Update Key must also be pre-configured at the master. The master may also have the USR pre-configured, but this is not strictly necessary. The master can obtain the USR by sending the outstation an Update Key Change Confirmation without an Update Key Change as described in 7.5.4.6.

5) The Update Key Change Method is configured at the master and sent to the outstation in the User Status Change object (g120v10). The User Status information supplied by the authority within that object must make use of the configured method. It is outside the scope of this standard whether the authority learns the correct Update Key Change Method from the master or vice versa.

Table 7-18- Configuration of Cryptographic Information

		Update Key Change Method							
		None		Symmetric			Asymmetric		
Information	**code**	**Master**	**Outstn**	**Auth**	**Master**	**Outstn**	**Auth**	**Master**	**Outstn**
Update Key Change Method		-	-	Note 5	Note 5	Rx	Note 5	Note 5	Rx
User Number	USR	Note 4	Config	-	Rx	Derive	-	Rx	Derive
Monitoring Direction Session Key		Derive	Rx	-	Derive	Rx	-	Derive	Rx
Control Direction Session Key		Derive	Rx	-	Derive	Rx	-	Derive	Rx
Update Key	K	Config	Config	Derive	Rx	Rx	Note 1	Derive	Rx
User Name	ID_A	-	-	Config	Rx	Rx	Config	Rx	Rx
Outstation Name	ID_B	-	-	Config	Config	Config	Config	Config	Config
Authority Certification Keys	M^C, B^C	-	-	Config	Config	Config	-	-	-
Authority Private Key	C’	-	-	-	-	-	Derive	-	-
Authority Public Key	C	-	-	-	-	-	Derive	Note 2	Config
User Private Key	A’	-	-	-	-	-	Note 3	Note 3	-
User Public Key	A	-	-	-	-	-	Note 3	Rx	Rx
Outstation Private Key	B’	-	-	-	-	-	-	-	Derive
Outstation Public Key	B	-	-	-	-	-	-	Config	Derive

Table 7-19: Legend for Configuration of Cryptographic Information

Cell Text	Meaning
Code	Notation for the information, found in 7.10.2
Auth	Authority
Outstn	Outstation
Derive	This device derives (creates) the information
Rx	This device receives the information via data communications
Config	This device must have this information pre-configured
-	This device does not use the information

7.6.1.5 Protocol Versions

The development of DNP Secure Authentication has required non-backward-compatible changes. The version of Secure Authentication described in IEEE 1815-2010 has been deprecated and should not be used in new implementations.

7.6.2 Options

This subclause describes capabilities that are not required for compliance with this standard, but may be implemented as options. If a device implements these capabilities, they shall be verified for compliance. If a device implements any capabilities not listed in this subclause, the device must provide a mode in which these capabilities are disabled.

7.6.2.1 MAC algorithms

7.6.2.1.1 AES-GMAC

Each device may optionally permit the use of the AES-GMAC algorithm, as described in NIST SP 800-38D, for authenticating data. If implemented, AES-GMAC shall be used in the following manner:

- No data shall be encrypted, i.e. this algorithm is AES-GMAC, not AES-GCM.
- The length of the output, known as the tag length, shall be 96 bits (12 octets).
- The length of the Initialization Vector (IV) shall also be 96 bits.
- The IV for each invocation of AES-GMAC shall be constructed as shown in Table 7-20, with the rightmost or most significant octets listed first in normal DNP fashion.
- The components (KSQ, SCS, CSQ) used to construct each IV shall come from the sources listed in Table 7-21, depending on the DNP object variation that contains the MAC. Table 7-21 also names which key is used to calculate the MAC in each object variation.

Table 7-20: Construction of AES-GMAC Initialization Vector

Field	Bits	Description
Fixed	8	Least significant octet of sender's DNP address
	8	Most significant octet of sender's DNP address
	16	User Number (USR) associated with the data being authenticated
Invocation	32	Key Change Sequence Number (KSQ) or Status Change Sequence Number (SCS)
	32	Challenge Sequence Number (CSQ) or zero

Table 7-21: Source of Initialization Vector Components in Each DNP Object

g120 Variation	Authentication Object Name	Initialization Vector		Key Used to Calculate MAC
		KSQ / SCS	CSQ	
2	Reply	Last KSQ sent by outstation	CSQ in this object	Session Key
5	Session Key Status	KSQ in this object.	Last CSQ exchanged between master and outstation, whether it was sent by the master in g120v3 or by the outstation in g120v1. Zero if neither exchange has happened yet.	Session Key. Note that if the Session Key is not valid, there is no MAC calculated.
9	Message Authentication Code	Last KSQ sent by outstation	CSQ in this same message (g120v3)	Session Key
10	User Status Change	SCS in this object	Zero.	Authority Certification Key
15	Update Key Change Confirmation	Last KSQ sent by outstation	Last CSQ exchanged between master and outstation, whether sent by master in g120v3 or by outstation in g120v1. Zero if neither exchange has happened yet.	Update Key

Note: While AES-GMAC offers enhanced efficiency in a MAC algorithm, it places some additional requirements on the implementation, particularly on the uniqueness of the Initialization Vector (IV). NIST SP 800-38D states that:

> *"The probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data shall be no greater than 2^{-32} . Compliance with this requirement is crucial to the security of GCM. Across all instances of the authenticated encryption [AES-GMAC] function with a given key, if even one IV is ever repeated, then the implementation may be vulnerable to the forgery attacks that are described in Ref [5] and summarized in Appendix A. In practice, this requirement is almost as important as the secrecy of the key."*

Table 7-20 describes what NIST SP800-38D defines as a "deterministic construction" of the IV. That specification also clarifies the previous statement by saying:

> *"For any given key, no two distinct devices shall share the same fixed field, and no two distinct sets of inputs [i.e. two messages] to any single device shall share the same invocation field."*

This strict requirement means that DNP Secure Authentication implementations that use AES-GMAC must implement the following rules in addition to those described elsewhere in this standard:

a) The most recently transmitted value of the Key Change Sequence Number (KSQ) shall be retained by both the master and the outstation over restarts.

b) The outstation shall not follow the usual rule, found in the object definition of (g120v5), that it must initialize the KSQ to zero after a restart. Instead, after a restart it shall increment the KSQ that was retained over the restart to create its first KSQ for transmission.

c) The master and the authority shall change the Update Key often enough that it occurs before the KSQ wraps around.

d) The DNP Address of each device shall be unique across the network administered by the key distribution authority. This is a difficult requirement for some DNP implementations, but it is vital if using the AES-GMAC algorithm. If this requirement cannot be met, then all keys (including Session Keys) used for calculating MACs must be unique across the network, a requirement which may be even more difficult to meet.

e) The Session Keys and Update Keys shall be changed frequently enough that AES-GMAC is used no more than 2^{21} times with the same key.

7.6.2.1.2 Other MAC algorithms

Each device may implement additional MAC algorithms in addition to those listed as mandatory. If the device receives an Error message with the Error Code <5> MAC algorithm Not Permitted, it shall change to use a mandatory MAC algorithm in its next Challenge. A device may be configured to reject particular mandatory MAC algorithms, but it must also support configuration to support all the mandatory MAC algorithms.

7.6.2.2 Key Wrap / Transport algorithms

7.6.2.2.1 AES-256 Key Wrap

Each device may optionally permit the use of the Advanced Encryption Standard Key Wrap mechanism, as described in IETF RFC 3394, to encrypt and decrypt Session Keys or Update Keys. If implemented, the Key Encryption Key (KEK) referred to in the Key Wrap specification shall be the Update Key, which shall be 256 bits long. The default initialization vector shall be used.

7.6.2.2.2 RSAES-OAEP

If the device implements an asymmetric Update Key Change Method using RSA algorithms as described in 7.6.1.4.9, it shall use the RSA Encryption Scheme with Optimal Asymmetric Encryption Padding (RSAES-OAEP) as described in IETF RFC 3447. The hash function used shall be either SHA-1or SHA-256 as listed in 7.6.1.4.9. The Mask Generation Function shall be MGF1 as described in IETF RFC 3447.

7.6.2.2.3 Other Key Wrap Algorithms

Each device may implement additional Key Wrap algorithms in addition to those listed as mandatory. If an outstation receives an Error message with the Error Code <6> Encryption Algorithm Not Permitted, it shall change to use a mandatory Encryption Algorithm in its next Key Status Message.

A device may be configured to reject particular mandatory encryption algorithms, but it must also support configuration to support all the mandatory encryption algorithms.

7.7 Special Applications

This subclause defines how this standard shall be applied in a few specific situations.

7.7.1 Use with the Internet Protocol Suite

DNP3 implementations over TCP/IP requiring confidentiality shall use both this application layer mechanism and the Transport Layer Security (TLS) internet standard as described in 7.8.

DNP3 implementations over UDP/IP shall use this application layer authentication mechanism by itself. Some implementations may choose to use other security measures (such as IPSec) along with this standard, but they are out of the scope of this standard.

Figure 7-30 illustrates the standard protocol profiles that are permitted using Secure Authentication. Shaded areas indicate security measures. Implementations that support the Confidential TCP profile shall also support the Authenticated TCP profile.

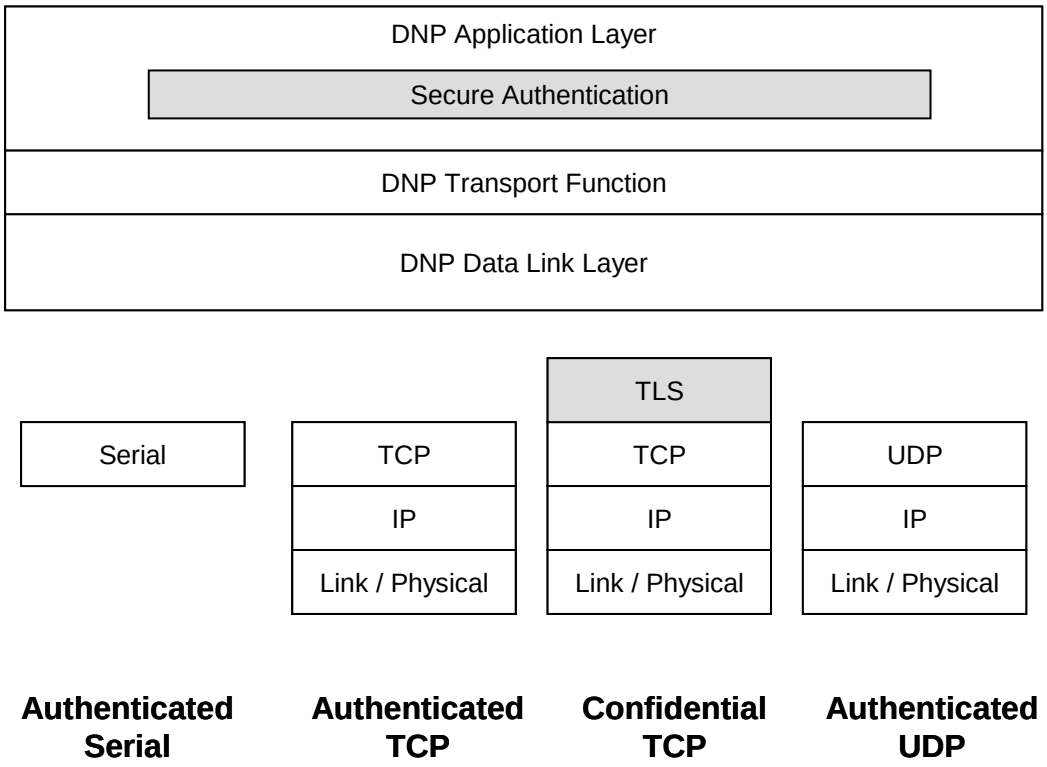


Figure 7-30: Valid Profiles Using the Secure Authentication Mechanism

When operating over IP, it may be possible to change and distribute Update Keys by making use of other IP-based security protocols. The DNP Users Group intends to develop specifications for this purpose. However, such mechanisms are also outside the scope of this standard as of the date of its publication.

NOTE: When operating over TCP, if the maximum number of authentication failures is exceeded, the implementation shall drop the TCP connection as specified in Table 7-8, in order to permit other connections to be made. It is also recommended that the event be logged and the Address Resolution Protocol (ARP) cache be cleared if possible.

7.7.2 Use with Redundant Channels

When used with redundant channels the communications shall not be considered to have failed and the Session Keys invalidated until all channels have been tried.

7.7.3 Use with External Link Encryptors

This authentication mechanism may be used along with external link encryptors to provide protection against the threat of eavesdropping.

It is recommended for simplicity that a common set of keys be used for both authentication and encryption. However, the definition of such rules is out of scope of this standard.

7.7.4 Use with Data Concentrators

This subclause describes special requirements when the authentication mechanism is used by a data concentrator.

7.7.4.1 Definition of a Data Concentrator

Figure 7-31 illustrates an example of a typical system making use of a DNP3 data concentrator. A data concentrator does not pass DNP3 messages through itself intact, as a router or bridge does. Instead, a data concentrator terminates multiple connections of DNP3 or other protocols and stores the data from each direction in an internal run-time database. This permits the concentrator to filter the data, process it within internal software applications, or convert it into other protocols.

Data may pass through a data concentrator either “upstream”, toward DNP3 masters, or “downstream”, toward DNP3 outstations, also known as Intelligent Electronic Devices (IEDs). DNP3 point numbers and DNP3 addresses used on any given connection may be the same or different than those used on any other connection. The data concentrator maps point numbers used on one connection to the corresponding point numbers on the other connections through the run-time database.

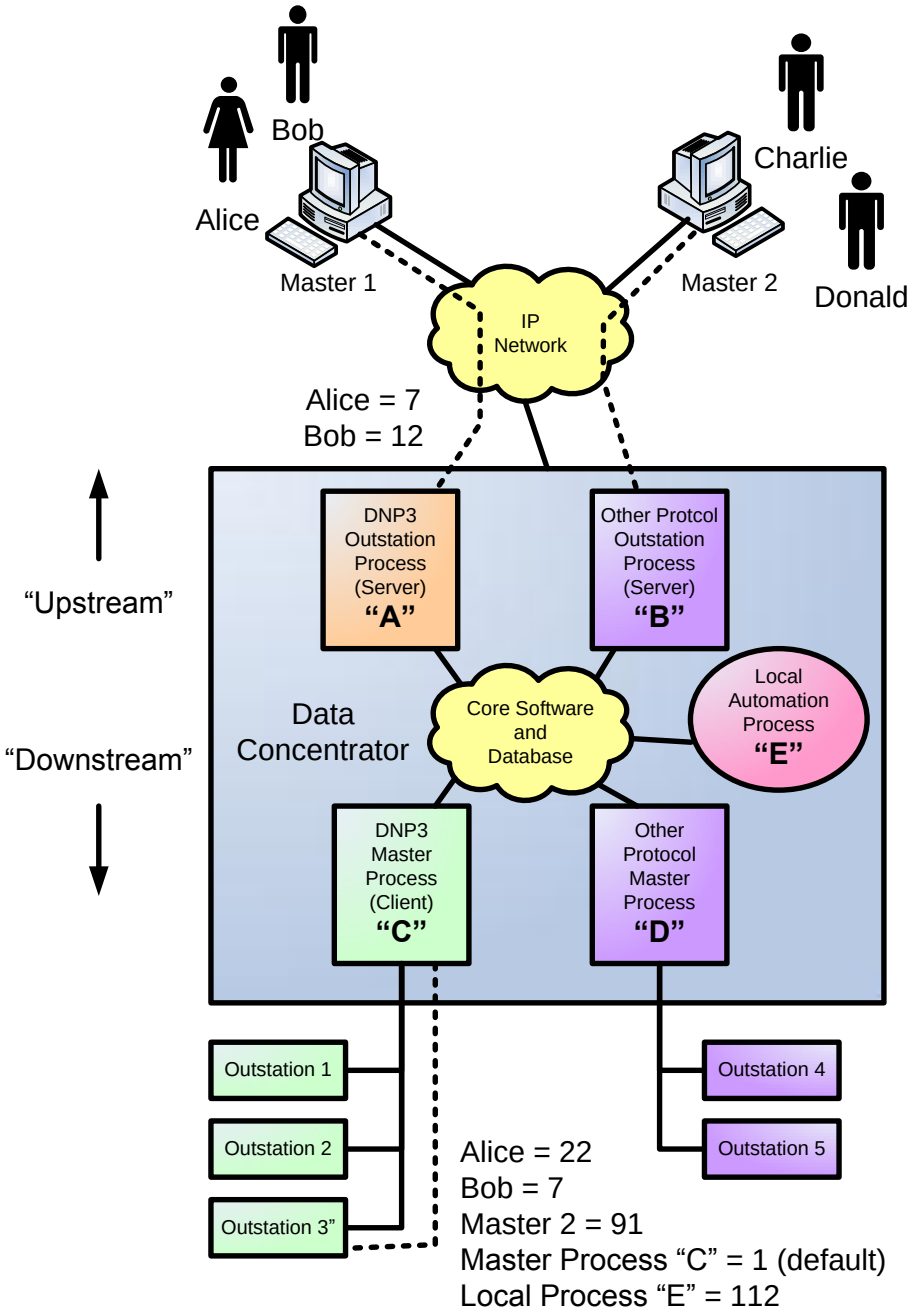


Figure 7-31: Example of User Number Assignments in a Data Concentrator

7.7.4.2 Authentication Procedures for Data Concentrators

When a data concentrator makes use of DNP3 secure authentication, it shall follow the general rule that whenever it can distinguish the particular user who initiated an operation, it shall identify that user to downstream outstations. This rule is intended to deter repudiation by permitting concentrators or outstations to log which user initiated critical DNP3 operations. The following rules shall apply as clarifications of that rule:

a) *The data concentrator shall identify each user having a DNP3 User Number (USR) on the upstream side with a separate DNP3 User Number on the downstream side.* For instance, in Figure 7-31, Alice and Bob have User Numbers on both the upstream DNP3 link used by process "A" and the downstream DNP3 links used by process "C".

b) *If an upstream protocol cannot distinguish individual users, the data concentrator shall identify each upstream protocol connection with a separate User Number on the downstream side.* For instance, process "B" cannot distinguish whether protocol commands are initiated by Charlie or Donald. Therefore the data concentrator uses a single User Number on the downstream DNP3 link used by process "C" to represent all users on Master 2.

c) *The data concentrator shall identify local users and applications with separate User Numbers on the downstream side.* For instance, local application "E" has its own User Number on the downstream DNP3 link. If the data concentrator had a local user interface capable of distinguishing different local users, it would identify each of these local users with a different User Number on the downstream DNP3 link.

d) *User Numbers shall be unique within a DNP association.* Refer to 7.5.4.4 for more details regarding this rule. User Numbers need not be sequential, but the combination of Association ID and User Number must uniquely identify a user within a device, and a unique Update Key and a set of Session Keys shall be associated with that user.

e) *The User Number used to identify a user on any given association may be different than that used on any other association.* For instance, Alice's User Number on the upstream DNP3 link is 7, but her User Number on the link between the data concentrator and Outstation 3 is 22. She may have a different User Number on the link with Outstation 1.

f) *If no points are mapped between an upstream or local user and a downstream outstation, the data concentrator need not map User Numbers either.* The Figure 7-31 illustrates that all the users identified in the diagram have the potential to make use of Outstation 3. However, not all users may have the potential to access Outstation 1, for instance, and therefore Outstation 1 may not have any User Numbers to distinguish them.

g) *When upstream or local users initiate critical DNP3 requests that are passed through to downstream outstations, the data concentrator shall correctly identify the user making the request.* If Alice initiates a binary output operation on a point that is mapped to Outstation 3, the data concentrator first authenticates the request with Master 1 using Alice's upstream User Number (7). Next, the data concentrator issues the corresponding binary output operation to Outstation 3, and it uses Alice's downstream User Number (22) when Outstation 3 requests the data concentrator to authenticate that request. Similarly, if the local automation process initiates a Freeze and Clear on several counters and Outstation 3 considers it a critical operation, the data concentrator shall authenticate the request with Outstation 3 specifying User Number 112.

h) *When the data concentrator spontaneously or periodically initiates a critical DNP3 request on behalf of multiple users, it shall identify itself as the user using the "default" User Number=1.* For instance, process "C" periodically initiates regular Class Data polls to gather data that will later be distributed to Alice, Bob and Charlie, even though none of those users specifically initiated the poll request. It is not mandatory that Class Data polls be considered critical. However, if Outstation 3 chose to challenge a Class Data poll from the data concentrator, the data concentrator would authenticate the poll identifying itself (User Number 1) as the initiating user.

7.8 Compliance with IEC 62351-3

DNP3 implementations that use Transport Layer Security (TLS) shall comply with the following requirements taken from IEC 62351-3. Italicized text is a direct quotation from Edition 1 of that specification.

7.8.1 Deprecation of Non-Encrypting Cipher Suites

Any cipher suite that specifies NULL for encryption shall not be used.

The list of deprecated suites includes, but is not limited to:

TLS_NULL_WITH_NULL_NULL

TLS_RSA_NULL_WITH_NULL_MD5

TLS_RSA_NULL_WITH_NULL_SHA

7.8.2 Mandatory Cipher Suite

DNP implementations that use TLS shall support the following cipher suite at a minimum:

TLS_RSA_WITH_AES_128_SHA

This is the mandatory cipher suite for TLS version 1.2.

7.8.3 Recommended Cipher Suites

It is recommended that DNP implementations using TLS support the following cipher suites. Implementations may also choose to implement cipher suites not listed here.

Table 7-22 Recommended Cipher Suite Combinations

Key Exchange		Encryption	Hash
Algorithm	Signature		
TLS_RSA_		WITH_RC4_128_	SHA
TLS_RSA_		WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_AES_128_	SHA
TLS_DH_	DSS_	WITH_AES_256_	SHA
TLS_DH_		WITH_AES_128_	SHA
TLS_DH_		WITH_AES_256_	SHA

7.8.4 Negotiation of Versions

Only TLS 1.0 corresponding to SSL version 3.1 (or higher) shall be allowable. Proposal of version prior to SSL 3.1 shall result in no connection being established.

7.8.5 Cipher Renegotiation

Implementations claiming conformance to this standard shall specify that the symmetric keys shall be renegotiated based upon a time period and a maximum allowed number of packets/octets sent. It is a PIXIT issue, of the referencing standard, to specify the constraints on the renegotiation.

The renegotiation values shall be configurable.

DNP implementations using TLS shall renegotiate the TLS symmetric keys when the application layer Session Key Change Interval expires or the Session Key Change Count is exceeded. It is recommended that TLS renegotiation take place before the application layer key change.

The initiation of the change cipher sequence shall be the responsibility of the TCP entity that receives the TCP-OPEN indication (e.g. the called entity). A request to change the cipher, issued from the calling entity (e.g. the node that issued the TCP-OPEN) shall be ignored,

There shall be a timeout associated with the response to a change cipher request. A timeout of the change cipher request shall result in the connection being terminated. The timeout value shall be configurable.

DNP implementations using TLS shall use a change cipher request timeout configurable in the same range as the application security reply timeout described in 7.6.1.4.1.

7.8.6 Message Authentication Code

The Message Authentication Code shall be used.

Note: TLS has this capability specified as an option. This standard mandates the use of this capability to aid in countering and detection of man-in-the-middle attacks.

7.8.7 Certificate Support

DNP Implementations using Transport Layer Security (TLS) shall comply with the following requirements for certificate management taken from IEC 62351-3.

7.8.7.1 Multiple Certificate Authorities (CAs)

An implementation, claiming conformance to this standard, shall support more than one Certificate Authority.

DNP Implementations using TLS shall support at least four Certificate authorities.

The actual number shall be declared in the implementation's Device Profile Document.

The criteria and selection of a CA is out-of-scope of this standard.

7.8.7.2 Certificate Size

A protocol, specifying the use of this standard, shall specify the maximum size of certificate allowed to be used. It is recommended that this size shall be less than or equal to 8192 octets.

DNP implementations using TLS shall support a minimum-maximum certificate size of 8192 octets. It is a local issue if larger certificates are supported.

An implementation that receives a certificate larger than the size that it can support shall terminate the connection.

7.8.7.3 Certificate Exchange

The certificate exchange, and validation, shall be bi-directional. If either entity does not provide its certificate, the connection shall be terminated.

7.8.7.4 Certificate Comparison

Certificates shall be validated by both the calling and called nodes. There are two mechanisms that shall be configurable for certificate verification.

- *Acceptance of any certificate from an authorized CA*
- *Acceptance of individual certificates from an authorized CA*

7.8.7.4.1 Verification based upon CA

An implementation, claiming conformance to this standard, shall be capable of being configured to accept certificates from one or more Certificate Authorities without the configuration of individual certificates.

7.8.7.4.2 Verification based upon individual Certificates

An implementation, claiming conformance to this standard, shall be capable of being configured to accept specific individual certificates from one or more authorized Certificate Authorities (e.g. configured).

7.8.7.4.3 Certificate Revocation

Certificate revocation shall be performed as specified in RFC 3280.

The management of the Certificate Revocation List (CRL) is a local implementation issue.

An implementation, claiming conformance to this standard, shall be capable of checking the local CRL at a configurable interval. The process of checking the CRL shall not cause an established connection to be terminated. An inability to access the CRL shall not cause the connection to be terminated.

Revoked certificates shall not be used in the establishment of a connection. An entity receiving a revoked certificate during connection establishment shall refuse the connection.

The revocation of a certificate shall terminate any connection established using that certificate.

Other standards, referencing this standard, shall specify recommended default evaluation intervals. The referencing standard shall determine the action that shall be taken if a certificate, currently in use, has been revoked.

DNP Implementations using TLS shall evaluate CRLs every twelve hours by default. The evaluation interval shall be configurable with hourly resolution. DNP devices shall terminate a connection when one of the certificates used to establish the connection is revoked.

Note: Through the normal application/distribution of CRL(s) connections may be terminated creating an inability to perform communications. Thus system administrators should develop certificate management procedures to mitigate such an occurrence.

7.8.7.4.4 Expired Certificates

The expiration of a certificate shall not cause connections to be terminated.

An expired certificate shall not be used or accepted during connection establishment.

7.8.7.4.5 Signing

Signing through the use of RSA or DSS algorithms shall be supported. Other algorithms may be specified in standards that reference this document.

7.8.7.4.6 Key Exchange

The key exchange algorithms shall support a maximum size of at least 1024 bits for the key.

Both RSA and Diffie-Hellman mechanisms shall be supported.

7.8.8 Co-existence with non-secure protocol traffic

Referencing standards shall provide a separate TCP/IP port through which to exchange TLS secured traffic. This will allow for the possibility of un-ambiguous secure and non-secure communications simultaneously.

DNP Implementations using TLS shall use the TCP port number 19999 by default to initiate secure connections.

DNP implementations using the application layer Secure Authentication mechanism but not TLS shall use port 20000 by default.

DNP implementations that do not use any security measures shall continue to use port 20000 by default as specified in the Networking volume.

Implementations that use other than the default TCP port numbers for DNP shall be configurable to use the defaults.

7.9 Compliance with IEC 62351-5

IEC 62351-5 states that protocols claiming compliance to it must include certain items in their specification. This subclause describes where in this standard those items are located.

7.9.1 Selected options

Application layer authentication security in DNP3 is provided through an implementation of the IEC 62351-5 standard. IEC 62351-5 states:

- *The protocol specification shall identify which of the options identified in clause 8.3* [IEC 62351-5] *are mandatory for the protocol (if any).*
- *The protocol specification shall identify any additional security algorithms, fixed parameters, configurable parameters or features supported by the protocol beyond the mandatory set specified in clause 8.2* [IEC 62351-5].

The Device Profile Document for each DNP3 device supporting IEC 62351-5 authentication shall identify this capability. Authentication is considered a subset of either master or outstation functionality to which a device may claim compliance, separate from any other subset.

All DNP3 devices shall support IEC 62351-5 Aggressive Mode authentication in order to claim compliance to IEC 62351-5 and DNP3. As noted in the specification, devices must also permit Aggressive Mode to be disabled via configuration.

All DNP3 devices shall permit the Error Count to be configurable.

The Device Profile Document for DNP3 devices claiming compliance with IEC 62351-5 shall also include the following information:

- A list of any and all hashing algorithms supported by the device in addition to the mandatory algorithms identified in IEC 62351-5.
- A list of any and all encryption algorithms supported by the device addition to the mandatory algorithms identified in IEC 62351-5.

7.9.2 Operations Considered Critical

IEC 62351-5 states:

- *The protocol specification shall identify which protocol operations (e.g. function codes, ASDU types, control commands, setting changes) shall be considered Critical, requiring authentication through this mechanism.*
- *The protocol specification shall specify that certain operations described in clause 7.3.3.2 of this specification* [IEC 62351-5] *are always Critical.*

The mandatory and optional critical operations for DNP3 are specified in 7.5.2.3.2.

7.9.3 **Addressing Information**

IEC 62351-5 states:

— *The protocol specification shall identify which addressing information from the lower layers of the protocol shall be included in the MAC calculation, as described in clauses 7.2.3.5 and 7.2.4.5, and the order of their octets in the calculation.*

DNP3 does not include any addressing information in the MAC calculation, as described in the Data Object Library insert sheets for Group 120.

7.9.4 **Message Format Mapping**

IEC 62351-5 states:

— *The protocol specification shall describe how each of the messages described in clause 7.2* [IEC 62351-5] *shall be implemented using the protocol.*

— *The message formats described in the protocol specification message formats shall include all information found in the messages described in this standard.*

— *In general, the protocol specification shall use the sequence, layout, and naming of information described in this standard. The only exception to this requirement occurs if an equivalent piece of information already exists elsewhere in a protocol ASDU (such as a length parameter). Under such conditions the format and layout described in this standard may be altered. Such a parameter shall not be removed from the protocol entirely.*

— *The timestamp included in the Error message shall be in a format defined by the protocol. This format shall represent an unambiguous absolute time, not a relative time, e.g. "milliseconds since midnight on the following date…" is acceptable, but not "milliseconds since the previous midnight".*

— *The protocol specification shall not reduce the size or range of any information described in this standard.*

The mapping of message formats is described in 7.5.1 and the Data Object Library for Group 120. Notes there describe how the length of challenge data and some other fields are implemented using DNP3 qualifier codes. The timestamp used is six-octet DNP absolute time.

7.9.5 **Reference to Procedures**

IEC 62351-5 states:

— *The protocol specification shall specify how the procedures described in clause 7.3* [IEC 62351-5] *shall be implemented using the protocol.*

— *If there is a disagreement between the procedures described in the protocol specification and the procedures described in this standard, this standard shall be deemed to be the correct description.*

The DNP3 procedures are described in 7.5.2 and are intended to be identical to those described in IEC 62351-5.

7.10 **Compliance with ISO/IEC 11770**

The methods for remotely changing Update Keys described in this document are based on the following international standards:

— ISO/IEC 11770-2:2008 Ed. 2: Key Establishment Mechanism 9 with 5-pass mutual authentication using a Key Distribution Centre and random numbers.

— ISO/IEC 11770-3:2008 Ed. 2: Key Transport Mechanism 3 with 2-pass mutual authentication; and Public Key Transport Mechanism 3: Public key distribution using a trusted third party.

This subclause describes how the steps described in these specifications have been implemented using the DNP3 objects described earlier in this document.

NOTE: While the DNP Secure Authentication mechanism is based on these standards, there are differences significant enough to make the DNP implementation non-compliant with ISO/IEC 11770. In particular, the encryption function specified by ISO/IEC 11770 for steps 7 and 8 in Table 7-24 has been replaced with a Message Authentication Code (MAC). This change was made to avoid sending the same information both encrypted and in the clear, while retaining the effectiveness of the authentication.

When comparing the process in this document with ISO/IEC 11770-3, it should be noted that the roles of "A" and "B" are reversed in the notation. In two of the exchanges, the role "M" for the DNP master is introduced, as distinct from "A", the user.

7.10.1 Requirements

This subclause describes the requirements defined when developing the method for remotely changing Update Keys that are described in this standard.

7.10.1.1 Functional Requirements

This subclause describes the functional requirements that must be met by the method for changing Update Keys.

7.10.1.1.1 Change Update Keys Remotely

The method shall permit utility personnel to change the Update Keys for any given user without traveling to remote sites.

7.10.1.1.2 Enable Centralized Key Management

The method shall permit Update Keys to be managed by a central authority within the utility. It shall permit a master station to distribute new Update Keys to an outstation, but prevent any entity associated with the master station from changing Update Keys without authorization from the central authority.

7.10.1.1.3 Permit Global Names

The method shall permit a user to be associated with a name that is unique across the utility. There shall be no technical limit to the length of this unique name.

7.10.1.1.4 Permit Assignment of Role-Based Access

The method shall permit a user to be assigned a particular role. An outstation may decide to enforce particular access privileges based on the assigned role. This document does not attempt to suggest what those roles may be.

7.10.1.1.5 Permit Revocation of Update Keys

The method shall permit the central authority to revoke the privileges of a user and therefore invalidate the Update Keys associated with that user. One way to do so would be to assign the user a role designated as "no longer valid".

7.10.1.1.6 Permit Expiry of Update Keys

The method shall permit the central authority to assign an expiry interval to a set of Update Keys, so that the outstation will consider the keys invalid after that interval.

7.10.1.1.7 Permit Assignment of User Number (USR)

The method shall permit the outstation to associate a short identifier, i.e. the User Number (USR) described in the DNP3 Secure Authentication specification, with the long, globally unique name provided for the user. The User Number shall be used for all subsequent authentication operations associated with this user. The method shall ensure that the master station authenticates this association operation.

7.10.1.1.8 Follow Standards

The method shall be based on international standards.

7.10.1.2 Qualitative Requirements

This subclause describes qualitative goals that the method should attempt to achieve.

7.10.1.2.1 Minimize Key Vulnerability

The method shall attempt to prevent keys from being compromised as much as possible.

7.10.1.2.2 Minimize Messages and Octets Required

The method shall attempt to use as few messages and octets as possible for the cryptographic technology used.

7.10.1.2.3 Minimize Configuration Required

The method shall attempt to use as little preconfigured information as possible for the cryptographic technology used. The preconfigured information required is described in detail in 7.6.1.4.10.

7.10.1.2.4 Minimize Processing Power Required

The method shall attempt to use as little processing power as possible.

7.10.2 Notation

The notation used for describing compliance with ISO/IEC 11770 is described in Table 7-23.

Table 7-23: Cryptographic Notation

Notation	Meaning
+	Concatenation within a message
[x]	The portion of the message known as “x” is optional
a	A particular user.
b	The outstation
c	A central authority trusted by both “a” and “b”. The equivalent of a certificate authority. Most likely to be some device, person or organization within the utility.
m	The DNP master, which acts on behalf of “a”.
A	a’s public key
A’	a’s private key
A^C	a’s symmetric key, shared between it and “c”.
B	b’s public key
B’	b’s private key
B^C	b’s symmetric key, shared between it and “c”.
C	c’s public key
C’	c’s private key
ID_A	A globally unique identifier representing the user “a”
ID_B	A globally unique identifier representing “b”
R_A	A random number chosen by “m” on behalf of “a”.
R_B	A random number chosen by “b”.
R_{MC}	A random number chosen by “m” for communication with “c”.
A(x)	“x” is encrypted with a’s public key
A’(x)	“x” is encrypted with a’s private key
$M^C(x)$	“x” is encrypted with the symmetric key shared between “m” and “c”.
B(x)	“x” is encrypted with b’s public key using a key transport scheme.
$B^C(x)$	“x” is encrypted with the symmetric key shared between “b” and “c”using a key wrap algorithm.
$S_A(x)$	“x” is digitally signed with a’s private key
$S_B(x)$	“x” is digitally signed with b’s private key
$S_C(x)$	“x” is digitally signed with c’s private key
K	The new Update Key to be used between “m” and “b” representing the user “a”.
$f_K(x)$	“x” is MACed using the Update Key, K
$f_C(x)$	“x” is MACed using the symmetric key shared between “b” and “c”.
K(x)	“x” is encrypted using a symmetric encryption algorithm and the Update Key, K.
USR	The shorthand user number chosen by “b” to represent the user “a” in all future communications.
KSQ	Key change sequence number chosen by “b” and kept the same throughout the message exchanges described here.
SCS	Status Change Sequence number managed by authority, unique between authority and outstation
Ack	Data identifying whether “b” accepted “a’s” authentication and change of the Update Key.
Role	Data indicating the role, e.g. operator, viewer, admin, config that “a” is to take.
Opr	Operation to be performed, i.e. Add, Delete, or change the specified Update Keys.
Interval	The length of time for which “c” will certify “a”.
CertA	Certificate for a’s public key, signed by “c”
CertB	Certificate for b’s public key, signed by “c”

7.10.3 **Sequence**

Table 7-24 uses the notation described in 7.10.2 to describe the DNP method in reference to ISO/IEC 11770. Note that steps 1, 5 and 6 are out of the scope of this standard.

Table 7-24: Compliance with ISO/IEC 11770

Step	Direction	Name	Method	Contents (Refer to the DNP3 Object Definitions for a complete list of parameters in the objects)	ISO/IEC 11770 Steps		Description
					Part 2 (Sym)	Part 3 (Asym)	
1	c → m	Change User Status by Authority	Asym Not DNP3	SCS + Opr + ID_A + Interval + Role + A + S_C(SCS + Opr + ID_A + Interval + Role + A)			The authority certifies that a particular user has been added, deleted, or its role has otherwise changed, for a specified interval.
			Sym Not DNP3	SCS + Opr + ID_A + Interval + Role + f_C(SCS + Opr + ID_A + Interval + Role)			
2	m → b	Change User Status (g120v10)	Asym	SCS + Opr + ID_A + Interval + Role + A + S_C(SCS + Opr + ID_A + Interval + Role + A)	n/a	12.2.1 A1 and B1	The master passes the certified status change information from the authority through to the outstation, without modification.
			Sym	SCS +Opr + ID_A + Interval + Role + f_C(SCS + Opr + ID_A + Interval + Role)	Not specified.	n/a	
3	m → b	Update Key Change Request (g120v11)	Both	ID_A + R_A	Not specified.	Not specified.	The master initiates the key change sequence by naming the user and providing random data.
4	m ← b	Update Key Change Reply (g120v12)	Both	KSQ + USR + R_B	7.3 (1) KSQ + USR added	11.4 A1 Text1 = KSQ+USR	The outstation challenges the master, assigns a User Number to the user, and assigns a Key Sequence Number.

Step	Direction	Name	Method	Contents (Refer to the DNP3 Object Definitions for a complete list of parameters in the objects)	ISO/IEC 11770 Steps		Description
					Part 2 (Sym)	Part 3 (Asym)	
5	c ← m	Request Key	Sym only, Not DNP3	$ID_A + R_{MC} + R_B + ID_B$	7.3 (2)	Not specified. Step 1 already provided a certificate.	In the symmetric case, the master requests the new Update Key from the authority.
6	c → m	Key for M and B	Sym only, Not DNP3	$M^C(ID_B + K + R_{MC}) + B^C(ID_A + K + R_B)$	7.3 (3) Text1 = null Text2 = null	Not specified. Step 1 already provided a certificate.	In the symmetric case, the authority provides the Update Key (K) to the master and authenticates the key change to both the master and outstation.
7	m → b	Update Key Change (g120v13)	Asym (g120v14)	$KSQ + USR + B(ID_A + K + R_B) + S_A(ID_B + R_A + R_B + KSQ + USR + B(ID_A + K + R_B))$	n/a	11.4 B1 Text2 = R_B Text3 = KSQ+USR Text4 = KSQ+USR	The master sends the new Update Key to the outstation, encrypted with the outstation's public key and authenticated by digitally signing with the user's private key.
			Sym (g120v15)	$KSQ + USR + B^C(ID_A + K + R_B) + f_K(ID_B + R_A + R_B + KSQ + USR)$	7.4 (4) Text2= null Text3=ID_B+ KSQ+USR Added KSQ+USR plain Uses an MAC instead of encryption	n/a	The master passes through the new Update Key to the outstation, encrypted with the symmetric key shared between the central authority and outstation, and authenticated using the Update Key itself.

Step	Direction	Name	Method	Contents (Refer to the DNP3 Object Definitions for a complete list of parameters in the objects)	ISO/IEC 11770 Steps		Description
					Part 2 (Sym)	Part 3 (Asym)	
7a.	m → b	Update Key Change Confirmation	Both. Optional instead of steps 5, 6 and 7. (g120v15)	f_K (ID_B + R_A + R_B + KSQ + USR)	7.4 (4) As above in step 7.		The master authenticates itself to the outstation and confirms which key is in use, but does not change the key. (optional instead of steps 5, 6 and 7)
8	m ← b	Update Key Change Confirmation	Both (g120v15)	f_K (ID_A + R_B + R_A + KSQ + USR)	7.4 (4) Text4=ID_A+ KSQ+USR Uses an MAC instead of encryption	Not specified.	The outstation confirms the key change and authenticates itself using the new Update Key.

11 DATA OBJECT LIBRARY—BASICS

11.5 DNP3 object types

11.5.6 Security Statistics Point type

11.5.6.1 General Description

Security statistics are used to monitor the use of the DNP3 secure authentication protocol described in Clause 7. Objects of this point type are used to count and report the number of times that particular events occur when two DNP3 devices are attempting to authenticate each other or to change cryptographic keys. The ability to monitor the number and frequency of errors and message exchanges during secure authentication provides an additional level of security. If certain statistics have large values or quickly increasing values, this may indicate an attack is underway.

Security statistics are monotonically increasing unsigned integer values. As such, they are essentially counters. However, security statistics differ from the counters described in 11.9.5 as described in Table 11-1.

Table 11-1: Security Statistics vs. Standard DNP3 Counters

Feature	Security Statistics	Standard DNP3 Counters
Source of Data	Incremented by the DNP3 software implementing the secure authentication specification.	May be incremented by software logic or external hardware events.
Point Numbers	Clause 7 specifies the use and meaning of particular point numbers for security statistics. Every DNP3 device that implements secure authentication shall use these point numbers and shall report all of the specified statistics. The point number used for the static and event objects refers to the same statistic.	The meaning of point numbers is left for the user to decide. The point number used for the static, frozen, and event objects refers to the same counter.
Variations	Always reported as 32-bit values with flag. Timestamp is optional.	May be reported in other variations.
Rollover	Statistics rollover to 0 after exceeding 4,294,967,295 and continue counting.	May rollover at other values.
Freezing and Clearing	Not permitted. Providing these features would create security vulnerabilities.	Optional.
Retention over Restarts	Device always retains the value in non-volatile memory over restarts.	Optional.
Event Reporting	Device generates events when the statistic exceeds a threshold.	Evaluation function determining when to generate an event is user-defined.
DNP Associations	Security statistics may be reported on a different DNP association than the one they are describing. For instance, master "B" may receive notification that the statistics for master "A" are reaching critical levels. Each device assigns a unique 16-bit Association ID for each DNP association. This ID is reported in the statistic object.	Apply only to the DNP association on which they are reported.

11.5.6.2 Security Statistics Model

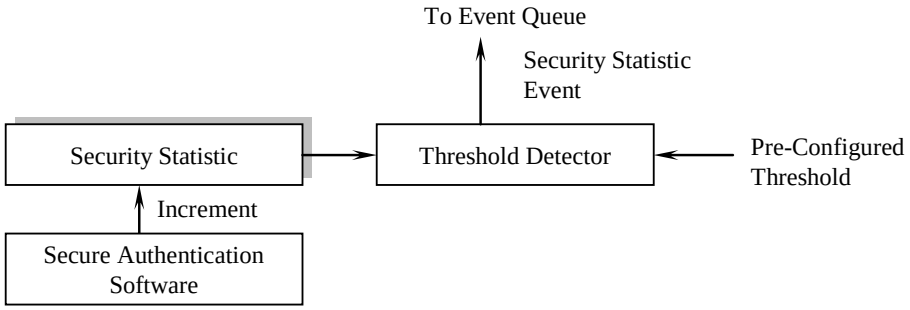


Figure 11-1: Security Statistics Model

The security statistics model is shown in Figure 11-1. The value of each statistic is incremented by the DNP3 software as described in Clause 7.

Each statistic has a pre-configured reporting threshold, similar to the deadbands for analog inputs. However, the statistic threshold cannot be set remotely as with analog inputs because that would create a potential vulnerability. Security statistics thresholds operate similar to fixed analog deadbands. Whenever the difference between the current value and the last reported value of a statistic exceeds the reporting threshold, the device generates an event. The value in the event becomes the last reported value. The default threshold for each statistic is specified in Clause 7.

There are other maximum thresholds for specific security statistics beyond the reporting thresholds. Their use is described in Clause 7.

11.5.6.3 Applicable DNP3 Objects

Table 11-2 shows which object groups are associated with security statistic point types. A specific point index number associated with any of these group numbers always references the same point.

Table 11-2: Security Statistics Point Type Object Groups

Group Number	Used For
121	Reporting the present value of a security statistic
122	Reporting security statistics events

ANNEX A. (NORMATIVE) DNP3 DATA OBJECT LIBRARY—OBJECT DESCRIPTIONS

A.45 Object Group 120: Authentication

A.45.1 Authentication—Challenge

DNP3 Object Library		Group:	120
		Variation:	1
Group Name:	Authentication	Type:	Info
Variation Name:	Challenge	Parsing Codes	Table 12-31

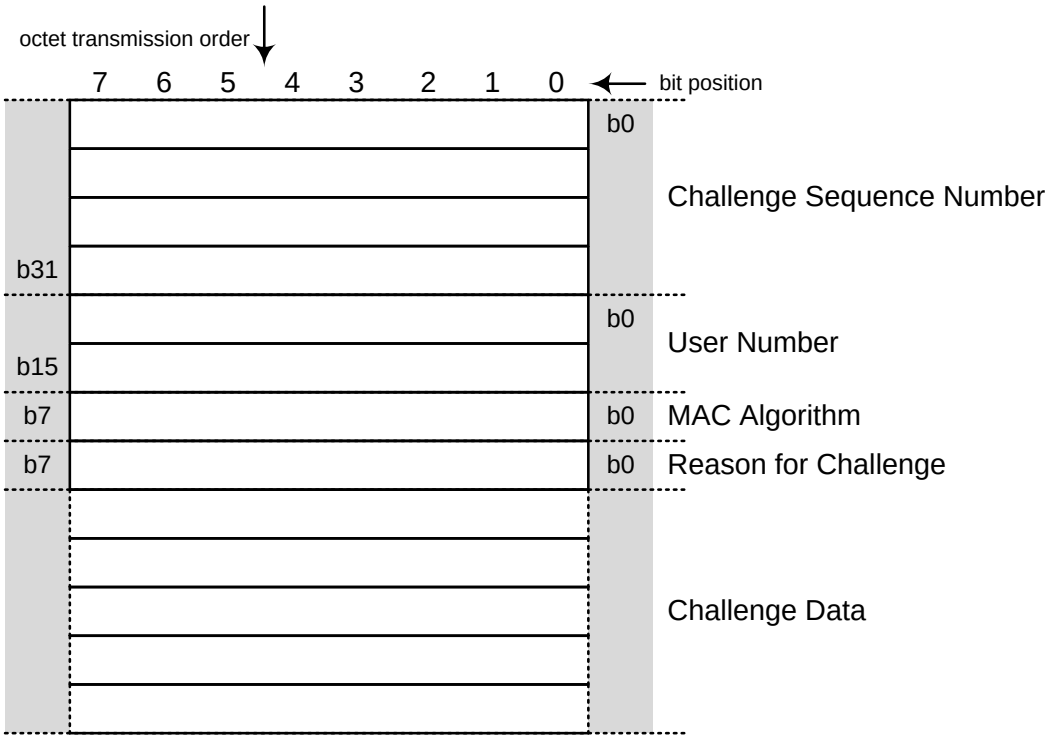
A.45.1.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object may be included in either a request or a response. When this object appears alone in the request or response its appearance requires that the other station (either master or outstation) transmit an Authentication Reply object with the MAC Value calculated based on this object and on the DNP3 fragment the other station most recently transmitted.

If the outstation transmits this object at the end of a response with the CON bit set, the outstation is requesting that the master transmit the application Confirm using aggressive mode authentication (g120v3 and g120v9).

A.45.1.2 Coding

A.45.1.2.1 Pictorial



A.45.1.2.2 Formal structure

UINT32: Challenge Sequence Number (CSQ).

Devices shall use this value to match Replies with challenges, according to the rules described in Clause 7.

UINT16: User Number (USR)

The responder shall use this value to identify which set of Session Keys is to be used in this challenge-response sequence.

<0> := Unknown. The challenge-response sequence is being initiated by an outstation. Therefore the appropriate USR is not yet known. The master will supply the appropriate USR in the Authentication Reply.

<1> := Default. The challenge-response sequence is being initiated by a master on behalf of more than one user, and the set of Session Keys used will therefore be the default set of keys for this master-outstation pair. Refer to the discussion in the supplement to Volume 2 for more information.

<2…65535> := Chosen by the master station to be associated with a particular user and corresponding set of Session Keys.

UINT8: MAC algorithm (MAL).

Using this value, the Challenger shall specify the algorithm that the Responder shall use to calculate the MAC Value, and shall also specify the resulting length of the MAC Value, Refer to 7.6.1.1 and 7.6.2.1and the references cited there for details of how to calculate these algorithms.

<0> := not used

<1> := HMAC SHA-1 truncated to 4 octets (serial). No longer recommended. USE ONLY FOR VERSION 2.0.

<2> := HMAC SHA-1 truncated to 10 octets (networked)

<3> := HMAC SHA-256 truncated to 8 octets (serial)

<4> := HMAC SHA-256 truncated to 16 octets (networked)

<5> := HMAC SHA-1 truncated to 8 octets (serial)

<6> := AES-GMAC (output is 12 octets)

<7..127> := reserved for future use

<128..255> := reserved for vendor-specific choices. Not guaranteed to be interoperable.

IMPORTANT: Refer to 7.6.1.4.3 regarding the dependency between the use of truncated HMAC algorithms and the need for frequent Session Key changes. In any case, the longest practical HMAC should be used; the shorter options are only provided to address performance issues on bandwidth-limited systems.

UINT8: Reason for Challenge.

This value explains the Challenger's reason for making the challenge. The Responder shall use this value to determine what extra data to include when calculating the MAC Value.

<0> := not used

<1> := CRITICAL. Challenging a critical function. The Responder shall include the entire *previous* ASDU transmitted by the Responder when calculating the MAC Value, as well as any further protocol-specific information.

<2..255> := reserved for future use

UINTn: Pseudo-Random Challenge Data.

Devices shall include pseudo-random data in the Challenge message to ensure that the contents of the Challenge message are not predictable. The pseudo-random data shall be generated using the algorithm 3.1 specified in FIPS 186-2. The minimum length of the Challenge Data shall be 4 octets.

A.45.1.2.3 Notes

In the DNP3 implementation of IEC 62351-5 authentication, the length of the Challenge Data is not specified within the object, but in the Object Prefix. The Authentication Challenge object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Challenge Data is therefore the size specified in the Object Prefix, minus 8 octets.

A.45.2 **Authentication—Reply**

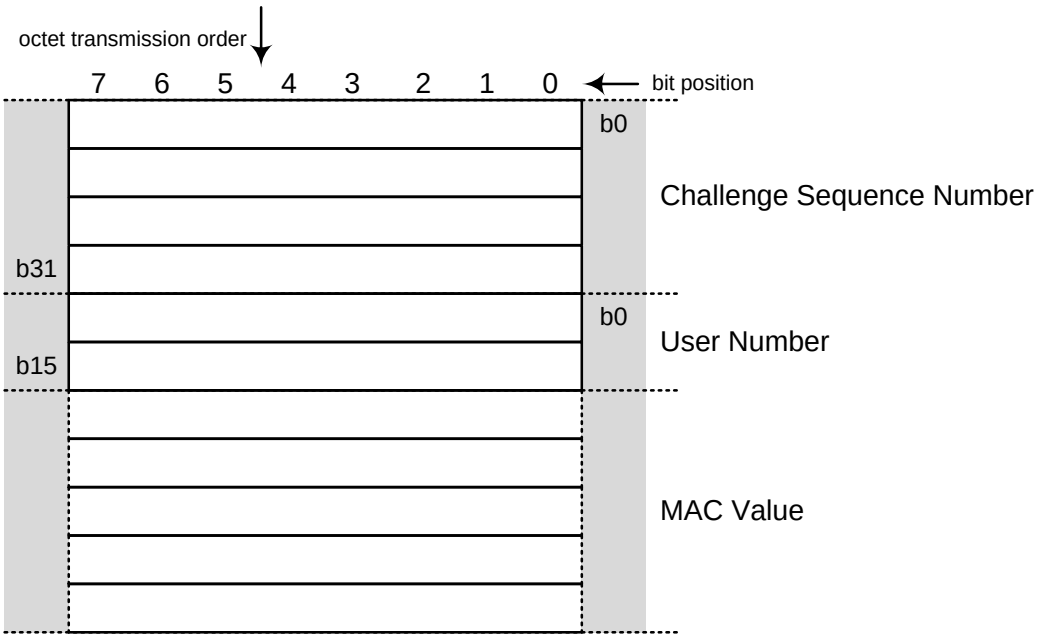
DNP3 Object Library		Group:	120
		Variation:	2
Group Name:	Authentication	Type:	Info
Variation Name:	Reply	Parsing Codes	Table 12-31

A.45.2.1 **Description**

This object is used for DNP3 secure authentication as described in Clause 7. This object may be included in either a request or a response. This shall be the only object to appear in the request or response. It is a reply to an Authentication Challenge object (g120v1).

A.45.2.2 **Coding**

A.45.2.2.1 **Pictorial**



A.45.2.2.2 **Formal structure**

UINT32: Challenge sequence number (CSQ).

The value transmitted in this object shall be the same value transmitted by the Challenger in the Authentication Challenge object.

UINT16: User Number (USR).

The sender shall use this value to identify which set of Session Keys the Challenger should use to authenticate this Reply. If the sender is the outstation, this value shall be the same as the USR value transmitted by the master in the previous Authentication Challenge message. If the sender is the master, it shall set the USR value according to which user is being authenticated. Refer to the discussion in Clause 7 for more information.

UINTn: MAC value.

The sender shall calculate the MAC Value according to the MAC algorithm specified by the Challenger, as described in Clause 7. The sender shall include in the MAC Value calculation the data listed in Table A-3, in the order listed.

Table A-3: Data included in the MAC value calculation

Data	Description	Included
Challenge message	The entire DNP3 Application Layer fragment containing the Authentication Challenge object.	Always.
Addressing information	Although IEC/TS 62351-5 specifies a protocol may include addressing information from lower layers, DNP3 authentication does not include any such addresses.	Never.
Challenged ASDU	The entire DNP3 Application Layer fragment being challenged, including the Application Layer header.	If the Reason For Challenging is <1>, challenging a critical function.
Padding Data	Any padding data required.	As required by the MAC algorithm.

Outstations sending this object shall use the current Monitoring Direction Session Key to calculate the MAC Value.

Masters sending this object shall use the current Control Direction Session Key to calculate the MAC value.

A.45.2.2.3 Notes

In the DNP3 implementation of IEC/TS 62351-5 authentication, the length of the MAC Value is not specified within the object but in the Object Prefix. The Authentication Reply object should always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65 535 octets, specified in the Object Prefix. The length of the MAC Value is therefore the size specified in the Object Prefix, minus 6 octets.

A.45.3 Authentication—Aggressive mode request

DNP3 Object Library		Group:	120
		Variation:	3
Group Name:	Authentication	Type:	Info
Variation Name:	Aggressive Mode Request	Parsing Codes	Table 12-31

A.45.3.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object may be included as the first object in either a DNP3 request or a DNP3 response. It attempts to authenticate the fragment it appears in.

Aggressive Mode must be preceded by a Challenge and a Reply. A device shall not transmit an Aggressive Mode Request until the device has received at least one Challenge message from the Challenger. Refer to the procedures in Clause 7 for more details.

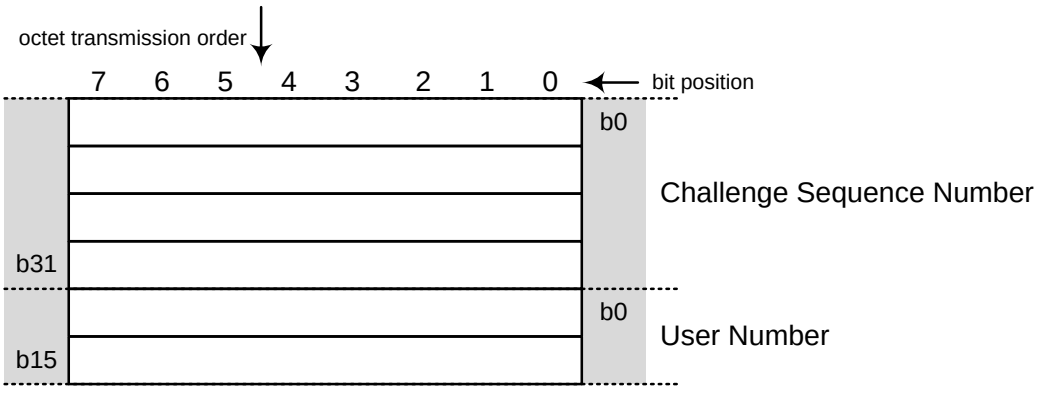
The initial Challenge is necessary because the sender of this object uses the data from the most recently received Challenge message to calculate the Challenge Sequence Number and the HMAC in the Aggressive Mode Request.

As shown in the following figure, the device shall include an Authentication HMAC object (g120v9) as the last object in the same fragment as the Authentication Aggressive Mode Request object.

Application Header	Object Header g120v3 Authentication Aggressive Mode Request	Object g120v3 Authentication Aggressive Mode Request	Object headers and objects to be authenticated, e.g. g12v1 Control Relay Output Block	Object Header g120v9 Authentication HMAC	Object g120v9 Authentication HMAC

A.45.3.2 Coding

A.45.3.2.1 Pictorial



A.45.3.2.2 Formal structure

UINT32: Challenge sequence number (CSQ).

The Challenge Sequence Number (CSQ) shall be the CSQ from the most recently received Challenge message, plus the number of Aggressive Mode Requests (g120v3) or Authentication Reply objects (g120v2) that the sender of this object has transmitted since receiving that Challenge message.

UINT16: User Number

The sender of this object shall use this value to identify which set of Session Keys is to be used to authenticate this Aggressive Mode Request.

<0> := Unknown. Not used for this object.

<1> := Default. One of two cases is occurring:

— This object is being sent by a master on behalf of more than one user.

— This object is being sent by an outstation and there is no corresponding user.

In either case, the set of Session Keys used will be the default set used for this master–outstation pair. Refer to Clause 7 for more information.

<2…65535> := Chosen by the master station to be associated with a particular user and corresponding set of Session Keys.

A.45.3.2.3 Notes

The DNP3 device shall transmit this object using the qualifier 0x07 (single-octet count of objects) with a count of 1.

A.45.4 Authentication—Session key status request

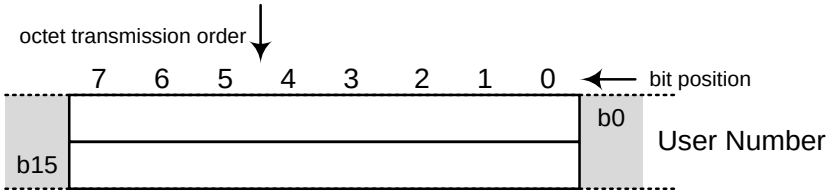
DNP3 Object Library		Group:	120
		Variation:	4
Group Name:	Authentication	Type:	Info
Variation Name:	Session Key Status Request	Parsing Codes	Table 12-31

A.45.4.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object may be included in a DNP3 request sent by the master only. This must be the only object to appear in the request. The function code to be used in this request is an Authentication Request (0x20). It is intended to elicit a DNP3 response with function code Authentication Response (0x83) containing a Session Key Status object.

A.45.4.2 Coding

A.45.4.2.1 Pictorial



A.45.4.2.2 Formal structure

UINT16: User Number

The master shall use this value to identify which set of Session Keys it is querying.

<0> := Unknown. Not used for this object.

<1> := Default. The default set of Session Keys used by the master on behalf of multiple users, or used when the outstation initiates the sequence of messages that results in an authentication. Refer to Clause 7 for a description of when this value should be used.

<2…65535> := Chosen by the master station to be associated with a particular user and corresponding set of Session Keys.

A.45.4.2.3 Notes

The master shall use the qualifier 0x07 (one octet count of objects) in the object header for this object.

A.45.5 **Authentication—Session key status**

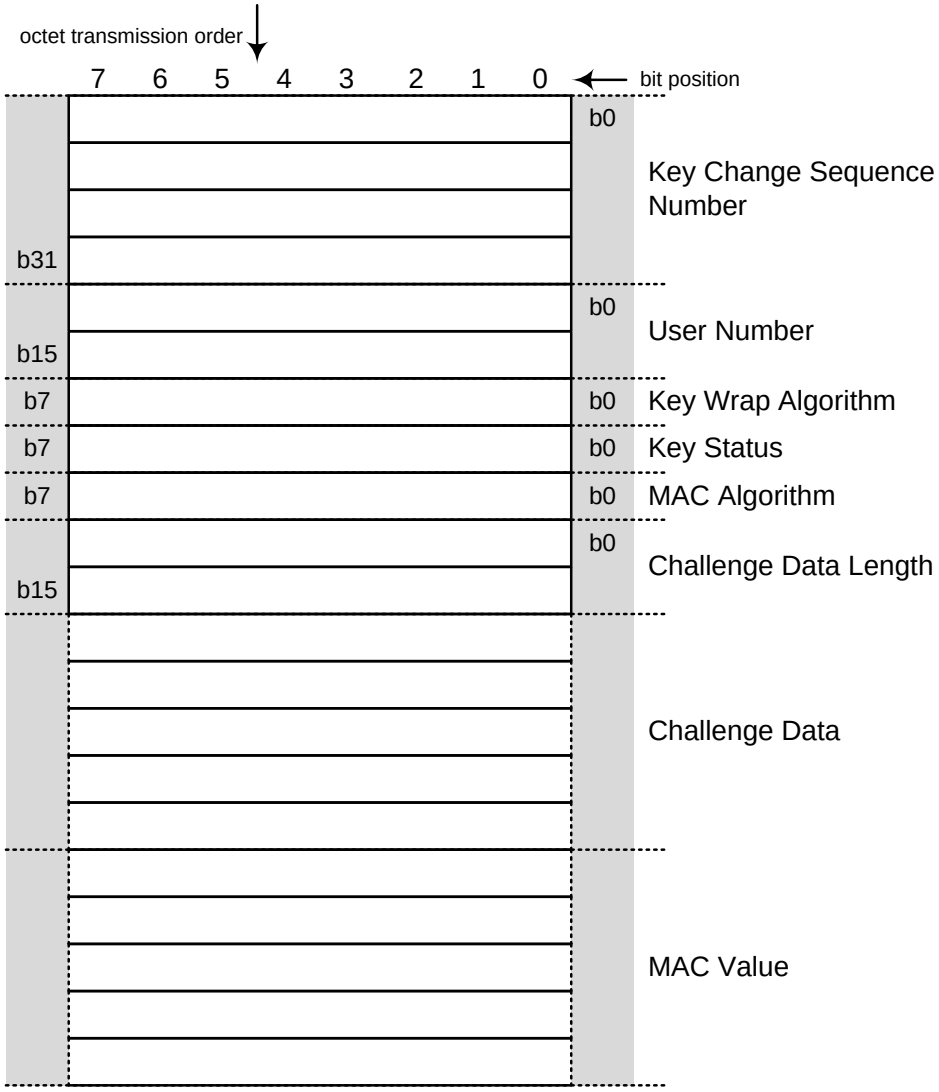
DNP3 Object Library		Group:	120
		Variation:	5
Group Name:	Authentication	Type:	Info
Variation Name:	Session Key Status	Parsing Codes	Table 12-31

A.45.5.1 **Description**

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 response only. This must be the only object to appear in the response. It is transmitted in response to a Session Key Status Request object and represents the current state of the Session Keys as known by the outstation. If the outstation considers the Session Keys to be valid, this object is authenticated with a MAC.

A.45.5.2 **Coding**

A.45.5.2.1 **Pictorial**



A.45.5.2.2 Formal structure

UINT32: Key Change Sequence Number (KSQ)

Each outstation shall maintain a Key Change sequence number, which it shall use to match Key Status messages with subsequent Key Change messages. This value shall be initialized to zero on start-up of the outstation (unless the MAC algorithm is AES-GMAC; see Clause 7). The outstation shall increment the KSQ each time it receives a Session Key Change or Session Key Status Request. (The first KSQ transmitted shall therefore always be 1) If the value reaches 4294967295, the next KSQ the outstation transmits shall be zero.

The master shall not process the KSQ except to include it in subsequent Key Change messages.

UINT16: User Number

The outstation shall use this value to identify the set of Session Keys for which it is reporting the current status. This value shall match the value supplied in the previous Session Key Status Request, as described in the definition of that object.

UINT8: Key wrap algorithm

Using this value, the outstation shall indicate to the master the algorithm it will use to decrypt the data in subsequent Session Key Change objects. Each device shall support at least the minimum subset of algorithms listed in Clause 7.

<0> := not used

<1> := AES-128 Key Wrap Algorithm, as described in 7.6.1.2.

<2> := AES-256 Key Wrap Algorithm, as described in 7.6.2.2.

<3..127> := reserved for future use

<128..255> := reserved for vendor-specific choices. Not guaranteed to be interoperable.

UINT8: Key status

This value describes the status of the two Session Keys as known by the outstation.

<0> := not used

<1> := OK. There have been no communications failures or restarts since the last time the outstation received an authentic Key Change message. The Session Keys are valid.

<2> := NOT_INIT. The outstation has not received an authentic Key Change message since it last started up, or has not received such a message within the Session Key Change Interval or Session Key Change Count configured at the outstation. The Session Keys are not valid.

<3> := COMM_FAIL. The outstation has detected a communications failure in either the control or monitoring direction. The Session Keys are not valid.

<4> := AUTH_FAIL. The outstation has received a non-authentic Challenge or Aggressive Mode Request. The Session Keys are not valid.

NOTE: This shall also be the response if the USR number supplied is invalid.

<5..255> := reserved for future use

UINT8: MAC algorithm (MAL).

Using this value, the outstation shall specify the algorithm that the master shall use to calculate the MAC Value, and shall also specify the resulting length of the MAC Value.

Refer to 7.6.1.1 and 7.6.2.1 and the references cited there for details of how to calculate these algorithms.

<0> := No MAC Value in this message.

<1> := HMAC SHA-1 truncated to 4 octets (serial)

<2> := HMAC SHA-1 truncated to 10 octets (networked)

<3> := HMAC SHA-256 truncated to 8 octets (serial)

<4> := HMAC SHA-256 truncated to 16 octets (networked)

<5> := HMAC SHA-1 truncated to 8 octets (serial)

<6> := AES-GMAC (output is 12 octets)

<7..127> := reserved for future use

<128..255> := reserved for vendor-specific choices. Not guaranteed to be interoperable.

IMPORTANT: Refer to 7.6.1.4.3 regarding the dependency between the use of truncated MAC algorithms and the need for frequent Session Key changes.

UINT16: Challenge Data Length

This value defines the length of the challenge data that follows.

UINTn: Pseudo-random challenge data

The outstation shall include this pseudo-random data in the Key Status message to verify that the contents of the Key Status message are not predictable. The pseudo-random data shall be generated using the algorithm specified in FIPS 186-2.

UINTn: MAC value.

The outstation shall calculate the MAC Value according to the MAC algorithm MAL, as described in Clause 7. The outstation shall include in the MAC Value calculation the data listed in Table A-4, in the order listed. It shall use the Monitoring Direction Session Key from the Session Key Change object most recently received from the master.

Note that this MAC is calculated regardless of whether the Session Keys are currently considered valid. If they are not valid, the outstation shall use the last Monitoring Direction Session Key that was considered valid. If there were no previous Session Keys, the MAL shall be <0> and there shall be no MAC value included in this object.

Table A-4: Data included in the MAC value calculation

Data	Description	Included
Challenge message	The entire DNP3 Application Layer fragment containing the Session Key Change object most recently received by the outstation.	Always.
Padding Data	Any padding data required.	As required by the MAC algorithm.

A.45.5.2.3 Notes

The Authentication Challenge object should always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65 535 octets, specified in the Object Prefix. The length of the Challenge Data may therefore be either calculated from the qualifier and the length of the HMAC or read from the corresponding field of the object.

A.45.6 Authentication—Session key change

DNP3 Object Library		Group:	120
		Variation:	6
Group Name:	Authentication	Type:	Info
Variation Name:	Session Key Change	Parsing Codes	Table 12-31

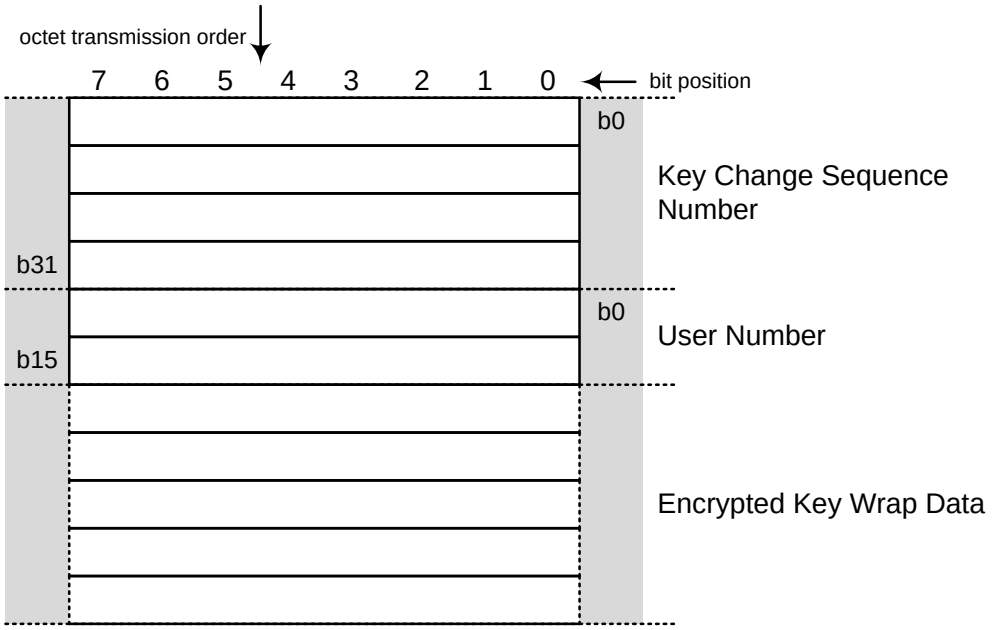
A.45.6.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. The master performs an Authentication Request (0x20) of this object to supply the outstation with the Session Key that will be used to calculate HMAC Values in all subsequent authentication operations. This must be the only object to appear in the request.

The Session Keys are encrypted using a separate Update Key.

A.45.6.2 Coding

A.45.6.2.1 Pictorial



A.45.6.2.2 Formal structure

UINT24: Key Change Sequence Number (KSQ)

This value shall match the KSQ transmitted in the Session Key Status object most recently received by the master, as described in the definition of that object.

UINT16: User Number (USR)

The master shall use this value to specify which set of Session Keys is to be changed. It shall match the USR in the Session Key Status object most recently received by the master, as described in the definition of that object.

UINTn: Wrapped key data

This value shall be the result of passing the Session Keys and the most recent Key Status message through the Key Wrap Algorithm defined in the Key Status message. The master shall pass the data through the Key Wrap Algorithm in the order described in Table A-5.

Table A-5: Data included in the key wrap (in order)

Data	Description	Included
Key Length	The size of one of the Session Keys. Both keys are the same length. This value is two octets long.	Always
Control Direction Session Key	The key used to authenticate data from the master.	Always
Monitoring Direction Session Key	The key used to authenticate data from the outstation.	Always
Key Status message	All data in the Session Key Status object most recently received from the outstation, KSQ first, not including any HMAC.	Always
Padding data	As required by the key wrap algorithm.	As required.

The Session Keys shall be treated as arrays of octets and transmitted with the lowest index octet first. For example, Appendix A of the AES specification provides the example of a 128-bit cipher key shown in Table A-6. The octet with index 0, having value 2b, shall be transmitted first.

Table A-6: Example of key order

Value	2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c
index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Note that the output from the key wrap algorithm may be longer than the input. For instance, the AES Key Wrap Algorithm produces output that is exactly 8 octets longer than its input. Table A-7 shows a typical example of the Wrapped Key Data using this algorithm.

Table A-7: Example of wrapped key data

Data	Description	Size (in octets)
Key Length	So the outstation will know what follows	2
Control Direction Session Key	Using the minimum size 128-bit keys	16
Monitoring Direction Session Key		16
Session Key Status object	Using the minimum size of challenge data, i.e. 4 octets	15
Padding data	Required to make the input data a multiple of 8 octets.	7
Additional output	For the AES key wrap algorithm	8
TOTAL		64

A.45.6.2.3 **Notes**

In the DNP3 implementation of IEC 62351-5 authentication, the length of the Wrapped Key Data is not specified within the object, but in the Object Prefix. The Authentication Key Change object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Wrapped Key Data is therefore the size specified in the Object Prefix, minus 6 octets.

The outstation should respond to this request with a Session Key Status Object (g120v5).

A.45.7 **Authentication—Error**

DNP3 Object Library		Group:	120
		Variation:	7
Group Name:	Authentication	Type:	Event/Info
Variation Name:	Error	Parsing Codes	Table 12-31

A.45.7.1 **Description**

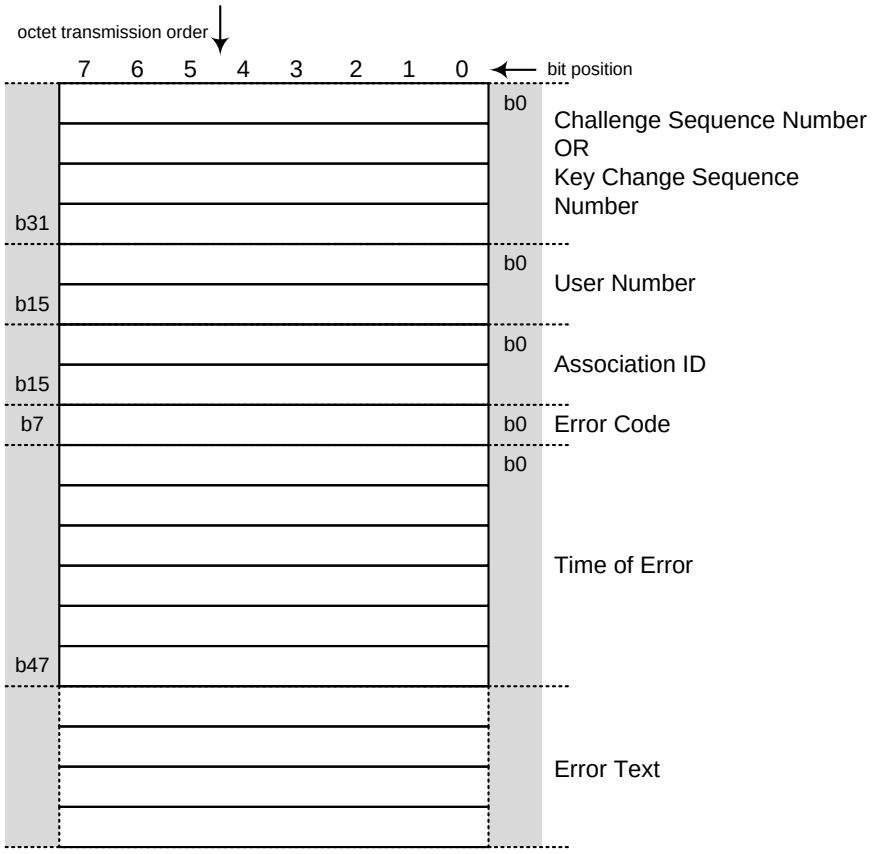
This object is used in DNP3 secure authentication as described in Clause 7. This object is used by a device (either master or outstation) to indicate an error with a previous authentication operation.

This object may be assigned to a Class and transmitted as an event object along with other data. Outstations shall not allow this object to be assigned to no class, or to static class 0. If sent by a master, this object is considered of type Info rather than Event.

It is recommended that an instance of each Authentication Error event object be created on each DNP3 association to an outstation. Doing so permits the outstation to report security problems on one association to masters on other associations. Note that the User Number must be unique within a DNP association, as described in the section of the supplement discussing data concentrators. Only the most recent Authentication Error event object shall be buffered; older event objects shall be discarded to avoid denial of service attacks.

A.45.7.2 Coding

A.45.7.2.1 Pictorial



A.45.7.2.2 Formal structure

UINT32: Sequence Number

This value shall be the Challenge Sequence Number or Key Change Sequence Number, of the operation that the Error message is replying to.

UINT16: User Number (USR)

This value shall be the User Number of the operation that the Error message is replying to, identifying the set of Session Keys and Update Key in use. Note that the User Number may also be zero when the correct User Number is unknown. Refer to Clause 7.

UINT16: Association ID

This value shall uniquely identify the association between the master and outstation on which the error occurred. The definition of a DNP association may be found in Clause13. Because of the variety of configurations of DNP implementations, the Association ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers or identifiers on the master and outstation. However, whatever mapping is used, the combination of User Number and Association ID shall be unique within the device.

UINT8: Error code.

This value shall specify the reason the error message is being transmitted.

<0> := not used

<1> := Authentication failed. The authentication information supplied by the other device was incorrect, or the data it was authenticating was corrupted in transit.

<2> := Unexpected response. The other device transmitted a message that did not follow the procedures as described in the supplement to Volume 2. NO LONGER SUPPORTED. USE ONLY FOR VERSION 2.0.

<3> := No response. The other device either did not respond to the Challenge message or did not follow an Aggressive Mode request with data for authentication. NO LONGER SUPPORTED. USE ONLY FOR VERSION 2.0.

<4> := Aggressive Mode not supported. The device sending this Error Code does not permit the use of Aggressive Mode on this link.

<5> := HMAC algorithm not supported. The device sending this Error Code does not permit the use of the specified HMAC algorithm on this link. Mandatory HMAC algorithms are specified in the supplement to Volume 2.

<6> := Key Wrap algorithm not supported. The device sending this Error Code does not permit the use of the specified Key Wrap algorithm on this link. Mandatory Key Wrap algorithms are specified in the supplement to Volume 2.

<7> := Authorization failed. The authentication information supplied by the other device was correct, but the authenticated user is not permitted to perform the requested operation.

<8> := Update Key Change Method not permitted. The outstation does not permit the specified key change method on this link. Mandatory Update Key Change Methods are specified in the supplement to Volume 2.

<9> := Invalid Signature. The digital signature supplied in a User Status Change or Signed Update Key Change object was invalid.

<10> := Invalid Certification Data. The Certification Data supplied in a User Status Change object was invalid.

<11> := Unknown User. The master attempted to change the Update Key of a user without first supplying a valid User Status Change.

<12> := Max Session Key Status Requests Exceeded. The master *on a different association* has requested Session Key Status too often and it is possible a denial of service attack is underway.

<13…127> := reserved for future standardization

<128..255> := private range for definition by each vendor. A device using this range shall use a different Error Code for each possible error reason, and shall supply an Error Text to explain each Error Code.

DNP3TIME: Time of error.

Time when the event occurred expressed in standard DNP3 time.

UNCDn: Error text.

This value shall be a string of text suitable for display on a user interface or in a security log encoded in unicode UTF-8 as described in IETF RFC 3629 (note that all characters encoded in 7-bit ASCII comply with UTF-8) . The Error Text shall explain the Error Code. It is recommended that the Error Text also include a unique description of the user represented by the User Number.

For standardized Error Codes, the Error Text is optional and the length of the text may be zero. For private range Error Codes, the Error Text shall be mandatory.

A.45.7.2.3 **Notes**

In the DNP3 implementation of IEC 62351-5 authentication, the length of the Error Text is not specified within the object, but in the Object Prefix. The Authentication Error object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Error Text is therefore the size specified in the Object Prefix, minus 15 octets.

The Error Text is optional.

A.45.8 Authentication—User Certificate

DNP3 Object Library		Group:	120
		Variation:	8
Group Name:	Authentication	Type:	Info
Variation Name:	User Certificate	Parsing Codes	Table 12-31

A.45.8.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 request only, using the Secure Authentication (0x20) function code. This must be the only object to appear in the request.

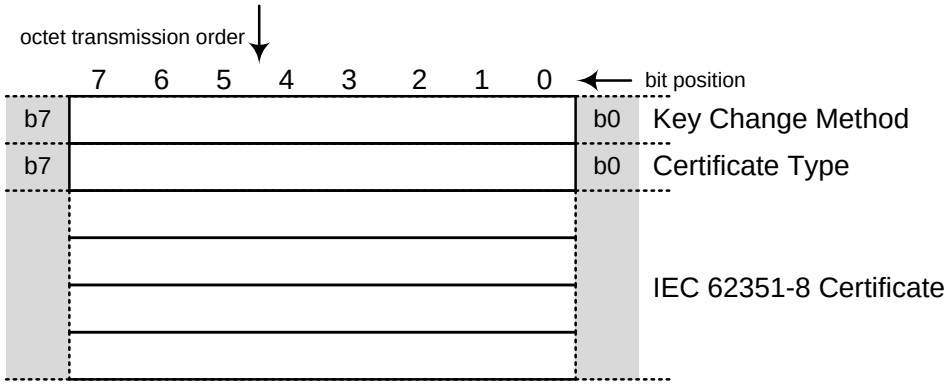
This object is transmitted by the master station to identify when a user of the outstation has been added or deleted, when the user's role has changed, or when the date has changed on which the user's access to the outstation will expire.

The data provided in this object is certified by an external authority that is not the master station itself. The authority provides the certificate to the master, and the master provides the certificate to the outstation without modification. The key used to sign the certificate shall be the private key of the authority.

This object variation is an alternate form of an Authentication User Status Change (g120v10) object. It is an extension of a standard X.509v3 certificate that carries the equivalent information to that found in g120v10. The master may transmit this object variation instead of g120v10. This object is only used with outstations that support asymmetric Update Key Change Methods.

A.45.8.2 Coding

A.45.8.2.1 Pictorial



A.45.8.2.2 Formal structure

UINT8: Key Change Method

The master shall use this value to identify the method that will be used to change the Update Keys associated with the user.

The possible values of Key Change Method are described in the supplement to Volume 2. Numbers less than 64 represent the use of symmetric keys and algorithms, while numbers 64 through 127 represent the use of mostly asymmetric (public) keys and algorithms. This object is not used with symmetric Key Change Methods.

<0..63> := Symmetric, not used with this object.

<64> := Obsolete. Do not use.

<65> := Obsolete. Do not use.

<66> := Obsolete. Do not use.

<67> := Asymmetric RSA-1024 / DSA SHA-1 / HMAC-SHA-1

<68> := Asymmetric RSA-2048 / DSA SHA-256 / HMAC-SHA-256-

<69> := Asymmetric RSA-3072 / DSA SHA-256 / HMAC-SHA-256

<70> := Asymmetric RSA-2048 / DSA SHA-256 / AES-GMAC

<71> := Asymmetric RSA-3072 / DSA SHA-256 / AES-GMAC

<72 ..127> := Reserved for future symmetric methods

<128..255> := Reserved for vendor-specific choices. Not guaranteed to be interoperable.

The algorithms identified here are described in more detail in the *Secure Authentication* supplement to Volume 2.

UINT8: Certificate Type

The master shall use this value to specify whether the IEC 62351-8 Certificate is an ID Certificate, which contains the user's public key, or an Attribute Certificate, which does not.

<0> := not used

<1> := ID Certificate

<2> := Attribute Certificate

<3..255 > := Reserved

UINTn: IEC 62351-8 Certificate

This data is an extension to a standard X.509v3 cryptographic certificate. The definition of an X.509v3 certificate is found in IETF RFC 5280. The format of this extension intended for use in the power industry is defined in IEC 62351-8. Parts of those specifications as they existed at the time of writing are reproduced here in order to explain the application to DNP3. However, if there is a disagreement between the text here and those specifications, those specifications are definitive.

IEFT RFC 5280 defines an X.509 ID Certificate in ASN.1 notation as follows:

```
   Certificate                                    ::=  SEQUENCE  {
        tbsCertificate                            TBSCertificate,
        signatureAlgorithm                        AlgorithmIdentifier,
        signatureValue                            BIT STRING  }

   TBSCertificate  ::=  SEQUENCE  {
        version                                   [0]          Version
must be v3,
        serialNumber
       CertificateSerialNumber,
        signature                                 AlgorithmIdentifier,
        issuer                                    Name,
        validity                                  Validity,
        subject                                   Name,
        subjectPublicKeyInfo                      SubjectPublicKeyInfo,
        issuerUniqueID                            [1]          IMPLICIT
UniqueIdentifier OPTIONAL,
                                                  -- If present, version

MUST be v2 or v3
```

```
        subjectUniqueID                         [2]          IMPLICIT
UniqueIdentifier OPTIONAL,
                                                -- If present, version
MUST be v2 or v3
        extensions                              [3]          EXPLICIT
Extensions OPTIONAL
                                                -- If present, version
MUST be v3
        }
```

IETF RFC 5755 also provides the following definition of an Attribute Certificate, which is used to change the role or other characteristics of a user without supplying the user's public key again.

```
AttributeCertificate ::= SEQUENCE {
          Acinfo                        AttributeCertificateInfo,
          signatureAlgorithm            AlgorithmIdentifier,
          signatureValue                BIT STRING
            }

AttributeCertificateInfo ::= SEQUENCE {
          version                       AttCertVersion -- version is
v2,
          holder                        Holder,
          issuer                        AttCertIssuer,
          signature                     AlgorithmIdentifier,
          serialNumber                  CertificateSerialNumber,
          attrCertValidityPeriod        AttCertValidityPeriod,
          attributes                    SEQUENCE OF Attribute,
          issuerUniqueID                UniqueIdentifier OPTIONAL,
          extensions                    Extensions OPTIONAL
            }

Attribute ::= SEQUENCE {
          Type                          AttributeType,
          values                        SET OF AttributeValue
                                        -- at least one value is
required
                            }

AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
```

At a minimum, a DNP3 device implementing this object shall support the following values in the *signatureAlgorithm* and *tbsCertificate.signature* of an ID Certificate, or the *signatureAlgorithm* and *acInfo.signature* fields of an Attribute Certificate (the two fields are always the same)

- *id-dsa-with-sha1*. To be used when the Key Change Method is <67>.
- *id-dsa-with-sha256.* To be used when the Key Change Method is <68> through <71>.

If a DNP3 device implementing this object is also to be compliant with IEC 62351-8, it must also support the following algorithms:

- *sha-1WithRSAEncryption*, key length 1024. To be used when the Key Change Method is <67>.
- *sha256WithRSAEncryption*,To be used when the Key Change Method is <68> through <71>, with the corresponding RSA key length.

This object shall contain the IEC 62351-8 extension to the X.509 certificate format, defined as follows:

```
  id-IEC62351 OBJECT_IDENTIFIER ::= { 1 2 840 10070 }

  id-IECuserRoles OBJECT_IDENTIFIER ::= id-IEC62351 { 8 1 }

  IECUserRoles ::= SEQUENCE OF UserRoleInfo

  UserRoleInfo ::= SEQUENCE { -- contains the role information blob
     -- IEC62351 specific parameter
      userRole                                SEQUENCE SIZE (1..MAX)
OF RoleID
      aor                                     UTF8String
(SIZE(1..64)),
      revision                                INTEGER (0..255),
      roleDefinition                          UTF8String (0..23)
OPTIONAL,
      -- optional fields to be used within IEEE 1815 and IEC60870-5
      operation                               Operation OPTIONAL,
      statusChangeSequenceNumber              INTEGER
(0..4294967295) OPTIONAL,
      }

  RoleId ::= INTEGER (-32768..32767)

  Operation ::= ENUMERATED { Add (1), Delete (2), Change (3) }
```

The *RoleID* numbers shall be the numbers defined in the User Status Change (g120v10) object for *User Role.* These have been chosen to correspond with the roles defined in IEC 62351-8. Note that this certificate format permits a particular user to be assigned multiple roles simultaneously, while the User Status Change object only permits a single role at a time.

The *aor* or Area of Responsibility field shall be used by the outstation to verify that this certificate applies to the outstation receiving the certificate. Area of Responsibility shall be a pre-configured characteristic of any outstation that uses this object. Defining possible values of this text string is the responsibility of the authority, but it may for instance indicate a geographical area or a portion of the organization. An outstation may belong to more than one Area of Responsibility. The outstation shall not accept any role changes for a user unless the *aor* field contains one of the Areas of Responsibility the outstation is configured to belong to.

The *revision* number shall always increase.

The *roleDefinition* is a string that is used to describe where the *RoleID* numbers have been defined. To comply with this standard, use the value “IEC62351-8” because the DNP3 *RoleID* numbers have been made to align with IEC 62351-8.

The other DNP3 Secure Authentication operating parameters discussed in this standard shall be included in the certificate as listed in Table A-8.

Table A-8: DNP3 Secure Authentication Parameters in IEC 62351-8 Certificates

DNP3 Parameter	Source in IEC 62351-8 ID Certificate	Source in IEC 62351-8 Attribute Certificate
User Name	*Certificate.tbsCertificate.subject*	*AttributeCertificate.Acinfo.holder*
User Public Key	*Certificate.tbsCertificate.* *subjectPublicKeyInfo*	Not included. Defined in the ID Certificate. An ID Certificate must be supplied by the authority before an Attribute Certificate can be used.
User Role Expiry Interval	*Certificate.tbsCertificate.validity* Subtract the *notBefore* time from the *notAfter* time to calculate the interval. If the outstation has secure time synchronization when it receives the certificate, it shall use the *notBefore* and *notAfter* times as provided. Otherwise, it shall use the calculated interval relative to the time it received the certificate. The outstations shall re-evaluate the expiry of the certificate whenever secure time synchronization is achieved.	*AttributeCertificate.Acinfo.* *attrCertValidityPeriod* As described for the ID certificate, but using the *notBeforeTime* and *notAfterTime* fields.
User Role	*Certificate.tbsCertificate.extensions.* *IECUserRoles.userRole* Note that there may be several instances of IECUserRoles, so multiple roles may be assigned to the user through one certificate.	*AttributeCertificate.Acinfo.extensions.* *IECUserRoles.userRole*
Operation	*Certificate.tbsCertificate.extensions.* *IECUserRoles.operation* Required in DNP3.	*AttributeCertificate.Acinfo.extensions.* *IECUserRoles.operation* Required in DNP3. Operation shall only be either (2) Delete or (3) Changes in an attribute certificate.
Status Change Sequence Number	*Certificate.tbsCertificate.extensions.* *IECUserRoles.* *statusChangeSequenceNumber* Optional if the authority can guarantee *Certificate.tbsCertificate.serialNumber* will always increase for this user.	*AttributeCertificate.Acinfo.extensions.* *IECUserRoles.* *statusChangeSequenceNumber* Optional if the authority can guarantee *AttributeCertificate.Acinfo.serialNumber* will always increase for this user.

A.45.8.3 **Notes:**

The Authentication User Certificate object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the IEC 62351-5 Certificate is therefore the length of the object minus one octet for the Key Change Method.

A.45.9 Authentication—Message authentication code (MAC)

DNP3 Object Library		Group:	120
		Variation:	9
Group Name:	Authentication	Type:	Info
Variation Name:	Message Authentication Code (MAC)	Parsing Codes	Table 12-31

A.45.9.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object may be included as the last object in either a DNP3 request or a DNP3 response. It attempts to authenticate the fragment it appears in.

Aggressive mode shall be preceded by a Challenge. A device shall not transmit an Aggressive Mode Request until it has received at least one Challenge message. Refer to the procedures in the *Secure Authentication* supplement for more details.

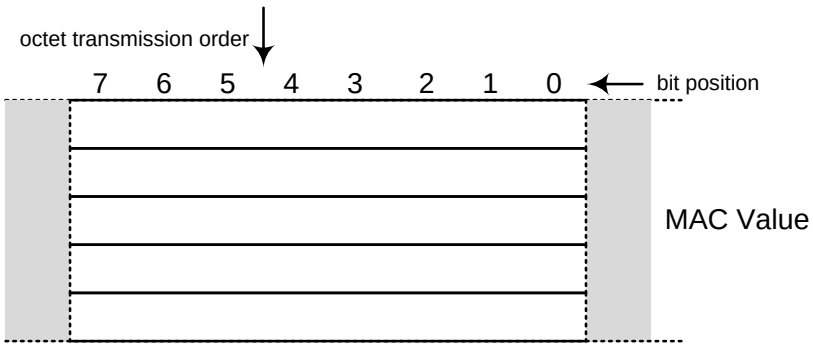
The initial Challenge is necessary because the sender of this object uses data from the most recently received Challenge message to calculate the MAC Value.

As shown in the following figure, the device shall include an Authentication Aggressive Mode Request object (g120v3) as the first object in the same fragment as the Authentication MAC object.

Application Header	Object Header g120v3 Authentication Aggressive Mode Request	Object g120v3 Authentication Aggressive Mode Request	Object headers and objects to be authenticated, e.g. g12v1 Control Relay Output Block	Object Header g120v9 Authentication MAC	Object g120v9 Authentication MAC

A.45.9.2 Coding

A.45.9.2.1 Pictorial



A.45.9.2.2 Formal structure

UINTn: HMAC Value

In aggressive mode, the MAC Value shall be calculated in the same manner as in normal mode, but shall be calculated based on the *same* ASDU as the Aggressive Mode Request, rather than the *previous* ASDU. Table A-9 describes this difference.

Table A-9: Data included in the HMAC value calculation in aggressive mode

Data	Description	Included
Challenge message	The entire DNP application layer fragment containing the most recently received Authentication Challenge Object, including the CSQ at the time of that challenge.	Always.
Addressing information	Although IEC 62351-5 specifies a protocol may include addressing information from lower layers, DNP3 authentication does not include any such addresses.	Never.
Authenticated Data	The entire DNP application layer fragment that this object is included in, including the application layer header, all objects preceding this one, and the object header and object prefix for this object.	Always.
Padding Data	Any padding data required.	As required by the MAC algorithm.

The length of the MAC value shall be determined by the MAC algorithm (MAL) of the most recent Challenge received by the sender of the object, as described in the definition of the Authentication Challenge object.

Outstations sending this object shall use the current Monitoring Direction Session Key to calculate the MAC Value.

Masters sending this object shall use the current Control Direction Session Key to calculate the MAC value.

A.45.9.3 Notes

In the DNP3 implementation of IEC/TS 62351-5 authentication, the length of the MAC Value is not specified within the object but in the Object Prefix. The Authentication Aggressive Mode Request object should be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65 535 octets, specified in the Object Prefix. The length of the MAC Value is therefore the size specified in the Object Prefix.

A.45.10 **Authentication—User Status Change**

DNP3 Object Library		Group:	120
		Variation:	10
Group Name:	Authentication	Type:	Info
Variation Name:	User Status Change	Parsing Codes	Table 12-31

A.45.10.1 **Description**

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 request only, using the Secure Authentication (0x20) function code. This must be the only object to appear in the request.

This object is transmitted by the master station to identify when a user of the outstation has been added or deleted, when the user's role has changed, or when the date on which the user's access to the outstation will expire has changed.

The data provided in this object is certified by an external authority that is *not* the master station itself. The authority provides the certification data to the master, and the master provides the certification data to the outstation without modification.

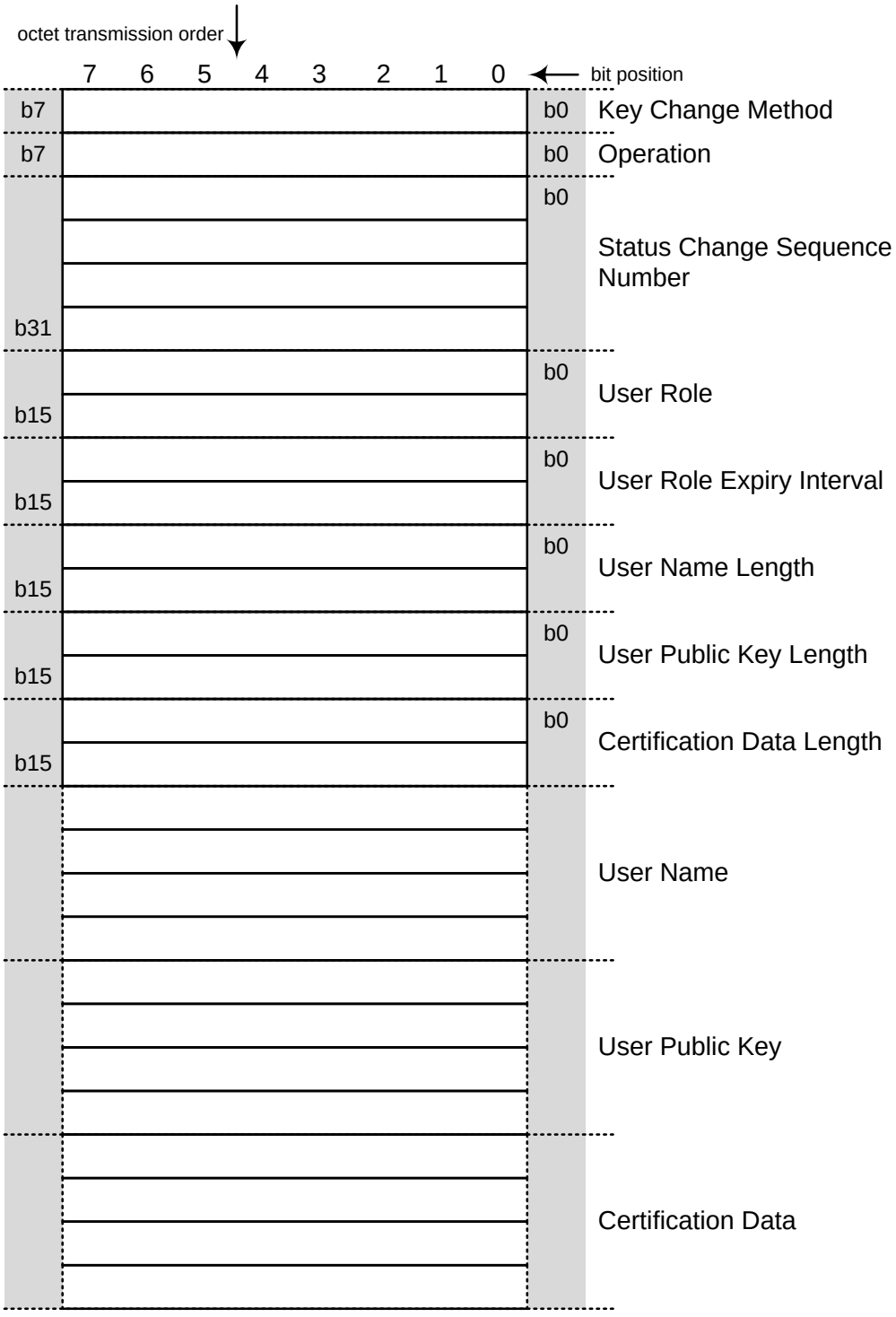
Prior to using this object, the choice to use either public keys or symmetric keys for remotely changing Update Keys shall be pre-configured at both master and outstation. This choice will determine the content of the Certification Data, as illustrated in Table A-10. Note that the Update Key Length (in octets) is transmitted in the symmetric case, but not the Update Key itself.

Table A-10: Creation of certification data

Method of Changing Update Keys	Public Keys	Symmetric Keys
User Status Information Included when producing the Certification Data (in order)	Operation Status Change Sequence Number User Role User Role Expiry Interval User Name Length User Public Key Length User Name User's Public Key	Operation Status Change Sequence Number User Role User Role Expiry Interval User Name Length User Name
Operation performed by the authority on the above Status Information to produce the Certification Data	Digital Signature	Message Authentication Code (note: not a Key Wrap algorithm – no key is transmitted in this case)

A.45.10.2 **Coding**

A.45.10.2.1 **Pictorial**



A.45.10.2.2 Formal structure

UINT8: Key Change Method

The master shall use this value to identify the method that will be used to change the Update Keys associated with the user. In this object, the Key Change Method specifies the operation the authority performed on the User Status Information to produce the Certification Data, and thus certify the user status change.

The possible values of Key Change Method are described in the supplement to Volume 2. Numbers less than 64 represent the use of symmetric keys and algorithms, while numbers 64 through 127 represent the use of mostly asymmetric (public) keys and algorithms.

<0> := not used

<1> := Obsolete. Do not use.

<2> := Obsolete. Do not use.

<3> := Symmetric AES-128 / SHA-1-HMAC

<4> := Symmetric AES-256 / SHA-256-HMAC

<5> := Symmetric AES-256 / AES-GMAC

<6..63> := Reserved for future symmetric methods

<64> := Obsolete. Do not use.

<65> := Obsolete. Do not use.

<66> := Obsolete. Do not use.

<67> := Asymmetric RS-1024 / DSA SHA-1 / SHA-1-HMAC

<68> := Asymmetric RSA-2048 / DSA SHA-256 / SHA-256-HMAC

<69> := Asymmetric RSA-3072 / DSA SHA-256 / SHA-256-HMAC

<70> := Asymmetric RSA-2048 / DSA SHA-256 / AES-GMAC

<71> := Asymmetric RSA-3072 / DSA SHA-256 / AES-GMAC

<72 ..127> := Reserved for future symmetric methods

<128..255> := Reserved for vendor-specific choices. Not guaranteed to be interoperable.

The algorithms identified here are described in more detail in the *Secure Authentication* supplement to Volume 2.

UINT8: Operation

The master shall use this value to specify how the user's status is to be changed:

<0> := not used

<1> := ADD. This is a new user not previously known to the outstation. The outstation shall record the User Status Information.

<2> := DELETE. The outstation shall invalidate the existing Update Key associated with the User Name.

<3> := CHANGE. The outstation shall update the User Status Information associated with the User Name.

<4..255> := reserved for future use

UINT32: Status Change Sequence Number (SCS)

The authority shall use this value to prevent replays of the User Status Change message. The authority shall set this value to 0 initially and increment it for each User Status Change. If the value is 4294967295, the next value shall be 0.

UINT16: User Role

The master shall use this value to identify the role the user is subsequently permitted to perform. No user is permitted to change the role of another user; only the authority may do so. Table A-11 describes the permitted standard roles and the corresponding permissions. The interpretation of these permissions is a local issue. Outstations may be configured to disallow any of the standard roles defined here.

Table A-11: User Role Definitions

Value	Name	Permissions						
		Monitor Data	Operate Controls	Transfer Data Files	Change Config	Change Security Config	Change Firmware	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	Yes	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..32767>	RESERVED	For future use.						
<32768..65535>	PRIVATE	Defined by external agreement. Not guaranteed to be interoperable.						

UINT16: User Role Expiry Interval

The master shall use this value to indicate when the role of this user will expire, causing the outstation to invalidate the Update Key associated with this User Name. This value shall indicate the number of days after receiving the User Status Change object that the outstation shall consider the user role to be expired. This value is not effective until after the user's Update Key has been changed following the User Status Change. Note that time synchronization is considered a mandatory Critical Function requiring authentication in DNP3.

UINT16: User Name Length

The master shall use this value to specify the length of the User Name that follows.

UINT16: User Public Key Length

The master shall use this value to specify the length (in octets) of the public key associated with this user.

— If the Key Change Method is less than 64, this value is zero. Note that the Update Key Length is included in the Certification Data as described in Table A-10 but the Update Key itself is not sent in this object.

— If the Key Change Method is between 64 and 127 inclusive, this value is the length of the User Public Key included in this object and signed by the authority.

— Any other values of Key Change Method are defined by external agreement and are not guaranteed to be interoperable.

UINT16: Certification Data Length

The master shall use this value to specify the total length of the Certification Data that follows.

UINTn: User Name

The master shall use this value to specify which user's status is to be changed. The name shall be unique within the organization managed by the authority, with one exception: the null-terminated UTF-8 string "Common" shall be used to indentify the common Update Key used between the master and the outstation. The format of the User Name is otherwise outside the scope of this standard.

UINTn: User Public Key

The master shall use this value to specify the Public Key associated with the user. Because it is a Public Key, it is not encrypted.

If symmetric keys are being used to change Update Keys (i.e. Key Change Method is < 64), there is no Public Key and this value is therefore not included in the object.

This value shall be an octet-by-octet copy of the *SubjectPublicKeyInfo* field from an X.509 certificate (IETF RFC 5280).

UINTn: Certification Data

The authority shall use this value to certify that the other fields of this object are correct. The authority shall create the Certification Data as described in Table A-10 using the specified Key Change Method and pass it to the master for verbatim transmission to the outstation in this field of this object.

A.45.10.3 **Notes:**

The Authentication User Status Change object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Certification Data may therefore be either calculated from the qualifier and the length of the other fields, or read from the corresponding field of the object.

A.45.11 **Authentication— Update Key Change Request**

DNP3 Object Library		Group:	120
		Variation:	11
Group Name:	Authentication	Type:	Info
Variation Name:	Update Key Change Request	Parsing Codes	Table 12-31

A.45.11.1 **Description**

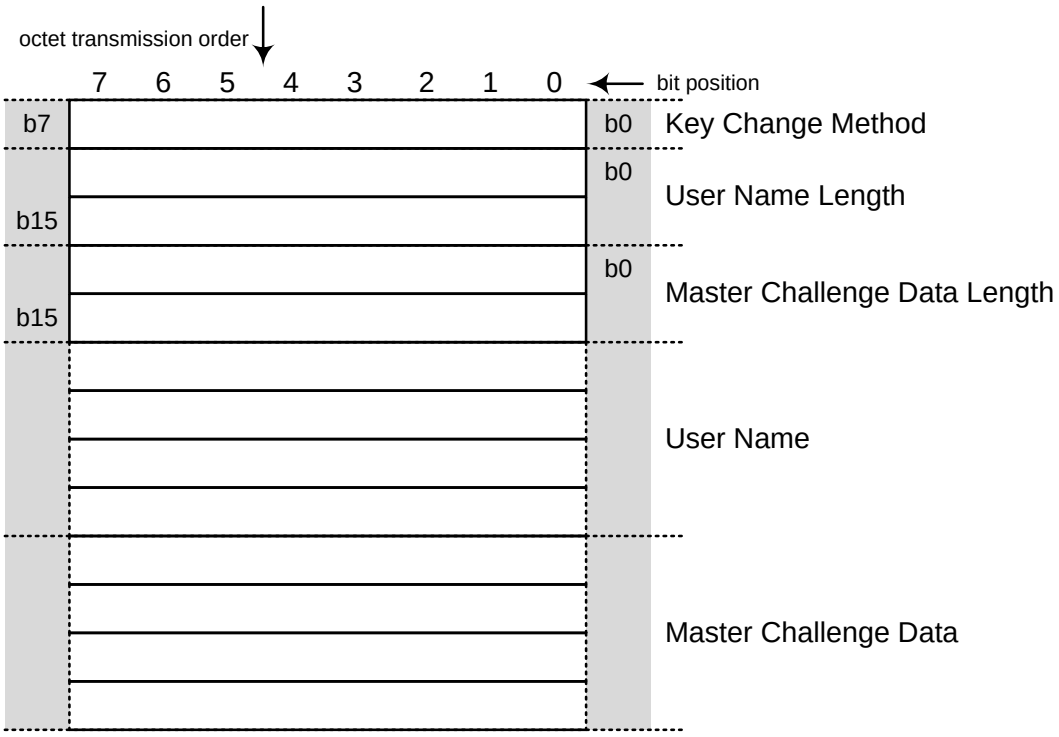
This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 request only, using the Authentication Request (0x20) function code. This must be the only object to appear in the request.

The master transmits this object to begin the process of changing the Update Key associated with a particular user at the outstation. The master specifies the name of the user whose Update Key is to be changed. The master also includes pseudo-random challenge data to be used by the outstation to authenticate itself.

The outstation shall send an Update Key Change Reply object in response to this object.

A.45.11.2 **Coding**

A.45.11.2.1 **Pictorial**



A.45.11.2.2 Formal structure

UINT8: Key Change Method

The master shall use this value to specify the method and algorithms (symmetric or asymmetric) that will be used to change the Update Key. The possible values of this field are described in the User Status Change object (g120v10). The master shall use numbers smaller than 64 to specify symmetric algorithms and keys and numbers 64 to 127 specify asymmetric algorithms and keys.

UINT16: User Name Length

The master shall use this value to specify the length of the User Name that follows.

UINT16: Master Challenge Data Length

The master shall use this value to specify the length of the challenge data that follows. The minimum length shall be as specified in Clause 7.

UINTn: User Name

The master shall use this value to specify which user's key is to be changed. The name shall be unique within the organization managed by the authority, with one exception: the null-terminated UTF-8 string "Common" shall be used to indentify the common Update Key used between the master and the outstation. The format of the User Name is otherwise outside the scope of this standard.

UINTn: Pseudo-random Challenge Data from Master

The master shall include this pseudo-random data in the Update Key Change Request if the Key Change Method is symmetric (less than 64). The pseudo-random data shall be generated using the algorithm 3.1 specified in the FIPS 186-2.

A.45.11.2.3 Notes

The Authentication Challenge object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix.

A.45.12 **Authentication— Update Key Change Reply**

DNP3 Object Library		Group:	120
		Variation:	12
Group Name:	Authentication	Type:	Info
Variation Name:	Update Key Change Reply	Parsing Codes	Table 12-31

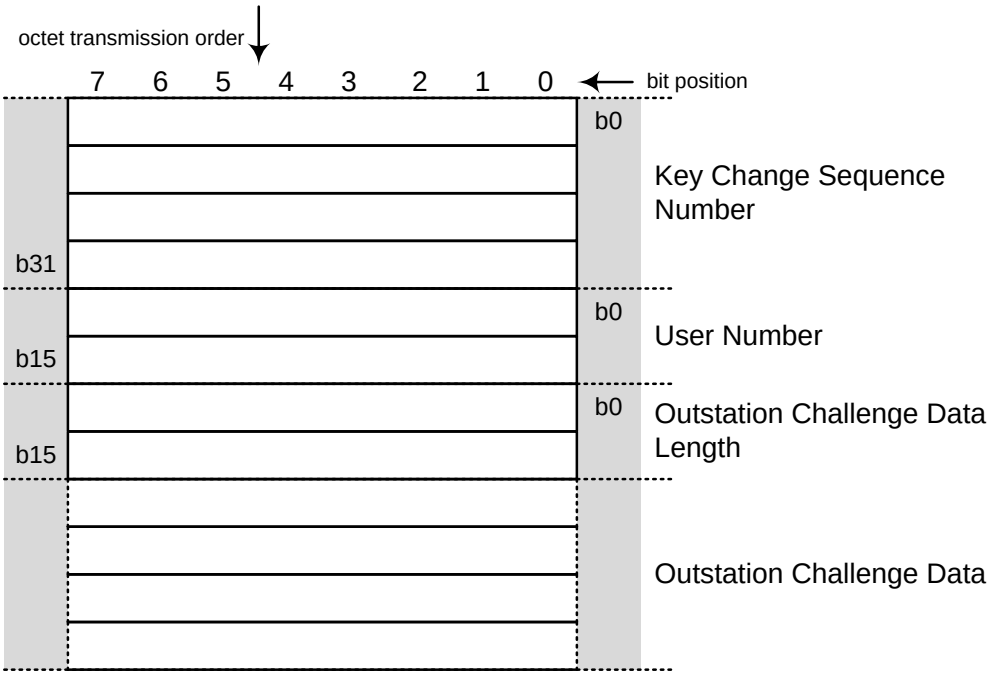
A.45.12.1 **Description**

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 response only, using the Authentication Response (0x83) function code.

This object is transmitted in response to an Update Key Change Request object. The outstation uses this object to assign a sequence number to the Update Key change sequence, assign a User Number to the user in question, and supply the master with pseudo-random challenge data.

A.45.12.2 **Coding**

A.45.12.2.1 **Pictorial**



A.45.12.2.2 **Formal structure**

UINT32: Key Change Sequence Number (KSQ)

This is the Key Change Sequence number defined in the Session Key Status object (g120v5). The outstation shall use this value to identify messages that are part of the same key change sequence. In addition to incrementing this value whenever it receives a Session Key Change or Session Key Status request, the outstation shall increment the KSQ each time it receives an Update Key Change Request object.

The master shall not process the KSQ except to include it in subsequent Update Key Change objects.

UINT16: User Number

This value is the integer value the outstation has chosen to represent the User Name specified in the Update Key Change Request object. The User Number need only be unique within the current DNP association between the master and the outstation.

UINT16: Challenge Data Length

This value defines the length of the challenge data that follows, in octets. The minimum length shall be as specified in the Secure Authentication supplement to Volume 2.

UINTn: Pseudo-random Challenge Data from Outstation

The outstation shall provide this pseudo-random data to ensure mutual authentication can take place between it and the master. The pseudo-random data shall be generated using the algorithm 3.1 specified in FIPS 186-2.

A.45.12.2.3 Notes

This object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Challenge Data may therefore be either calculated from the qualifier, or read from the corresponding field of the object.

A.45.13 **Authentication— Update Key Change**

DNP3 Object Library		Group:	120
		Variation:	13
Group Name:	Authentication	Type:	Info
Variation Name:	Update Key Change	Parsing Codes	Table 12-31

A.45.13.1 **Description**

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 request only.

The master uses this object to supply the encrypted new Update Key for the user.

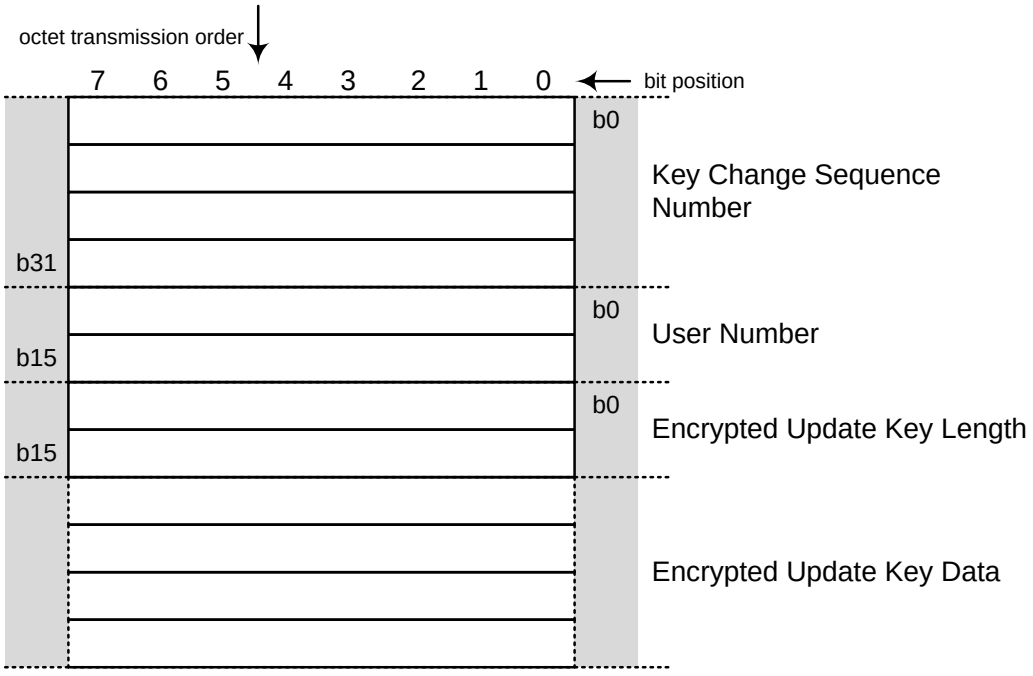
This object shall be followed in the same DNP3 request by one of the following objects based on the Update Key Change Method specified by the master in the Update Key Change Request.

— If the Update Key Change Method is symmetric, an Update Key Change Confirmation object (g120v15) follows.

— If the Update Key Change Method is asymmetric, an Update Key Change Signature object (g120v14) follows.

A.45.13.2 **Coding**

A.45.13.2.1 **Pictorial**



A.45.13.2.2 Formal structure

UINT32: Key Change Sequence Number (KSQ)

This is the Key Change Sequence number supplied by the outstation in the Update Key Change Reply object (g120v12).

UINT16: User Number

This value is the integer value the outstation has supplied in the Update Key Change Reply object (g120v12) to represent the user whose Update Key is being changed.

UINT16: Encrypted Update Key Length

This value defines the length of the encrypted Update Key that follows.

UINTn: Encrypted Update Key Data

This value contains the new Update Key for the user, plus the name of the user and the Outstation Challenge Data from the outstation, in the order shown in Table A-12.

Table A-12: Encrypted Update Key Data

Data	Description	From object…
User Name	The organizationally-unique name of the user associated with the new Update Key	Update Key Change Request
Update Key	The new Update Key for the user	
Outstation Challenge Data	Pseudo-random data selected by the outstation	Update Key Change Reply
Padding Data	Any padding data required	n/a

The Update Key Data shall be encrypted using the algorithm specified in the Key Change Method of the Update Key Change Request.

The Update Key Data shall be encrypted using one of the following keys:

— *If the Key Change Method is symmetric, the Update Key Data shall be encrypted using the symmetric key shared between the central authority and the outstation. The master shall pass this Encrypted Update Key Data from the central authority to the outstation in this object without modification.*

— *If the Key Change Method is asymmetric, the Update Key Data shall be encrypted using the outstation's public key.*

A.45.13.2.3 Notes

This object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix.

A.45.14 Authentication— Update Key Change Signature

DNP3 Object Library		Group:	120
		Variation:	14
Group Name:	Authentication	Type:	Info
Variation Name:	Update Key Change Signature	Parsing Codes	Table 12-31

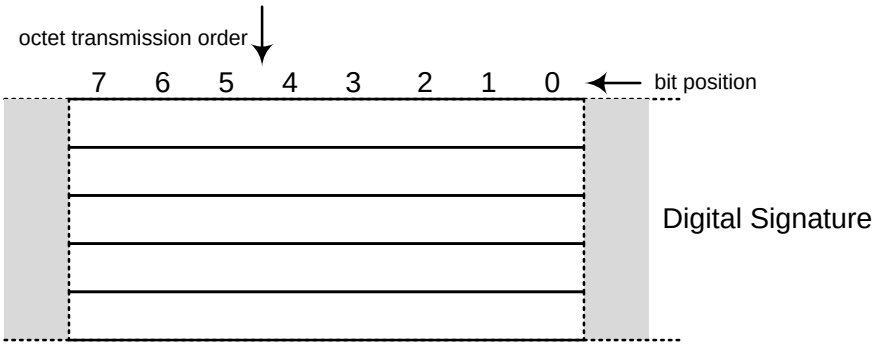
A.45.14.1 Description

This object is used for DNP3 secure authentication as described in Clause 7. This object is included in a DNP3 request only, following an Update Key Change object (g120v13). This object authenticates the changing of the Update Key for a particular user.

This object shall be transmitted by the master only when the master specified a Key Change Method in its most recent Update Key Change Request that specifies the use of asymmetric (public) keys and algorithms (i.e. the value of Key Change Method was between 64 and 127).

A.45.14.2 Coding

A.45.14.2.1 Pictorial



A.45.14.2.2 Formal structure

UINTn: Digital Signature

This value is the digital signature of the master on behalf of the user, calculated over the data found in Table A-13 in the order shown, using the algorithm specified in the Key Change Method of the Update Key Change Request.

The master shall calculate the signature using the Private Key of the user, corresponding to the Public Key the master supplied in the User Status Change (g120v10) object.

Table A-13: Data Included in the Digital Signature

Data	Description	Source
Outstation Name	The organizationally-unique name of the outstation.	Pre-configured
Master Challenge Data	Pseudo-random data selected by the master	Update Key Change Request
Outstation Challenge Data	Pseudo-random data selected by the outstation	Update Key Change Reply
Key Change Sequence Number (KSQ)	Sequence number that stays the same for this set of key change messages	Update Key Change Reply
User Number (USR)	Short number assigned by the outstation to represent this user	Update Key Change Reply
Encrypted Update Key Data	The encrypted Update Key and accompanying data, including the name of the user associated with the Update Key	Update Key Change
Padding Data	Any padding data required.	n/a

A.45.14.2.3 **Notes**

This object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix.

A.45.15 Authentication— Update Key Change Confirmation

DNP3 Object Library		Group:	120
		Variation:	15
Group Name:	Authentication	Type:	Info
Variation Name:	Update Key Change Confirmation	Parsing Codes	Table 12-31

A.45.15.1 Description

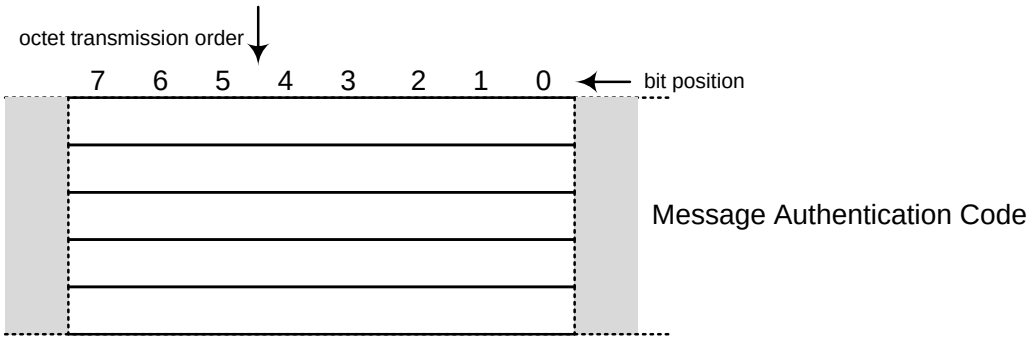
This object is used for DNP3 secure authentication as described in Clause 7. This object may be included in either a DNP3 request or a DNP3 response. It authenticates the master and outstation to each other using a message authentication code (MAC) and the new Update Key that is supplied by the master.

Exchanging this object ensures that both master and outstation agree on the following information:

- The new Update Key
- The name of the user or outstation who is receiving the object.
- The pseudo-random challenge data provided by both master and outstation to avoid replay
- The sequence number identifying this Update Key Change
- The User Number that will be associated with this Update Key in all subsequent authentications

A.45.15.2 Coding

A.45.15.2.1 Pictorial



A.45.15.2.2 Formal structure

UINTn: Message Authentication Code (MAC)

Table A-14 describes the authentication data to be used in the calculation, in the order shown. Although similar data is transmitted in both directions, it is important that the name of the sender and the order of the pseudo-random data in the calculation differ depending on the direction. This prevents an attacker from replaying the data sent by one device to impersonate the other device.

The key used to calculate the MAC is the new Update Key supplied by the master in the Update Key Change object. The algorithm and length of the MAC shall be determined by the Key Change Method field of the Update Key Change Request that initiated this key change sequence.

Table A-14: Data Included in the MAC Calculation

Data	Description	From object…
Receiver's User Name	Long organizationally-unique name for the user or outstation whose is receiving this object.	If a master is receiving this object, this name comes from the Update Key Change Request
		If an outstation is receiving this object, the outstation name was pre-configured.
Sender's Challenge Data	If a master is sending this object, this is the Master Challenge Data	Update Key Change Request
	If an outstation is sending this object, this is the Outstation Challenge Data	Update Key Change Reply
Receiver's Challenge Data	If a master is receiving this object, this is the Master Challenge Data	Update Key Change Request
	If an outstation is receiving this object, this is the Outstation Challenge Data	Update Key Change Reply
Key Change Sequence Number (KSQ)	Sequence number that stays the same for this set of key change messages	Update Key Change Reply
User Number	Short number assigned by the outstation to represent this user	Update Key Change Reply
Padding Data	Any padding data required.	n/a

A.45.15.2.3 **Notes**

This object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65535 octets, specified in the Object Prefix. The length of the Encrypted Authentication Data is therefore the size specified in the Object Prefix.

A.46 Object Group 121: Security statistics

A.46.1 Security statistic—32-bit with flag

DNP3 Object Library		Group:	121
		Variation:	1
Group Name:	Security Statistic	Type:	Static
Variation Name:	32-bit with flag	Parsing Codes	Table 12-31

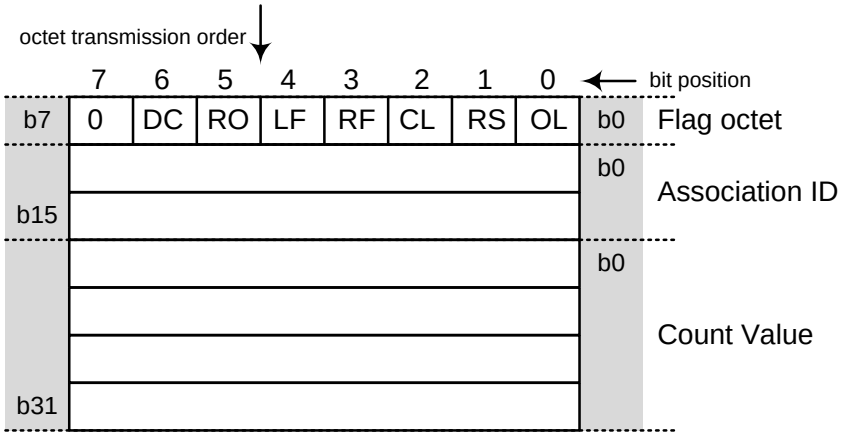
A.46.1.1 Description

This object is used to report the current value of a security statistic. See 11.5.6 for a description of a Security Statistic Point Type. Clause 11 specifies the point numbers permitted for this object and describes when the statistics are incremented.

Variation 1 objects contain a 32-bit, unsigned integer count value.

A.46.1.2 Coding

A.46.1.2.1 Pictorial



A.46.1.2.2 Formal structure

BSTR8: Flag Octet

Bit 0:	ONLINE
Bit 1:	RESTART
Bit 2:	COMM_LOST
Bit 3:	REMOTE_FORCED
Bit 4:	LOCAL_FORCED
Bit 5:	ROLLOVER
Bit 6:	DISCONTINUITY
Bit 7:	Reserved, always 0.

UINT16: Association ID

This value shall uniquely identify the association between the master and outstation on which the statistic is measured. The definition of a DNP association may be found in Clause 13. Because of the variety of configurations of DNP implementations, the Association ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers or identifiers on the master and outstation. The Association ID shall be unique within the device. A value of 0 for Association ID means the statistic was measured on the same association on which this object is reported.

UINT32: Count value

This is the most recently obtained or computed value.

Range is 0 to +4294967295.

A.46.1.2.3 Notes

See 11.6 for flag bit descriptions.

A.47 Object Group 122: Security statistic events

A.47.1 Security statistic event—32-bit with flag

DNP3 Object Library		Group:	122
		Variation:	1
Group Name:	Security Statistic Event	Type:	Event
Variation Name:	32-bit with flag	Parsing Codes	Table 12-31

A.47.1.1 Description

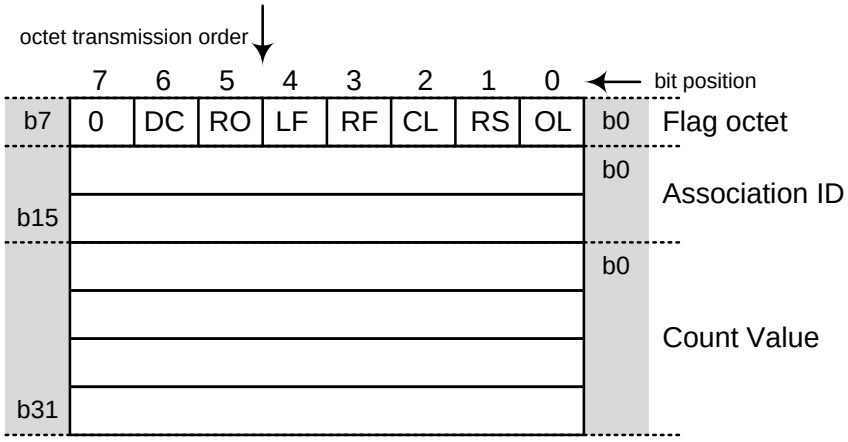
This object is used to report the value of a security statistic after the count has changed. See 11.5.6 for a description of a Security Statistic Point Type. Clause 11 specifies the point numbers permitted for this object and describes when the statistics are incremented.

Outstations shall not allow this object to be assigned to no class, or to static class 0.

Variation 1 objects contain a 32-bit, unsigned integer count value.

A.47.1.2 Coding

A.47.1.2.1 Pictorial



A.47.1.2.2 Formal structure

BSTR8: Flag Octet

Bit 0:	ONLINE
Bit 1:	RESTART
Bit 2:	COMM_LOST
Bit 3:	REMOTE_FORCED
Bit 4:	LOCAL_FORCED
Bit 5:	ROLLOVER
Bit 6:	DISCONTINUITY

Bit 7: Reserved, always 0.

UINT16: Association ID

This value shall uniquely identify the association between the master and outstation on which the statistic is measured. The definition of a DNP association may be found in Clause 13. Because of the variety of configurations of DNP implementations, the Association ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers or identifiers on the master and outstation. The Association ID shall be unique within the device. A value of 0 for Association ID means the statistic was measured on the same association on which this object is reported.

UINT32: Count value

This is the most recently obtained or computed value.

Range is 0 to +4294967295.

A.47.1.2.3 Notes

See 11.6 for flag bit descriptions.

A.47.2 Security statistic event—32-bit with flag and time

DNP3 Object Library		Group:	122
		Variation:	2
Group Name:	Security Statistic Event	Type:	Event
Variation Name:	32-bit with flag and time	Parsing Codes	Table 12-31

A.47.2.1 Description

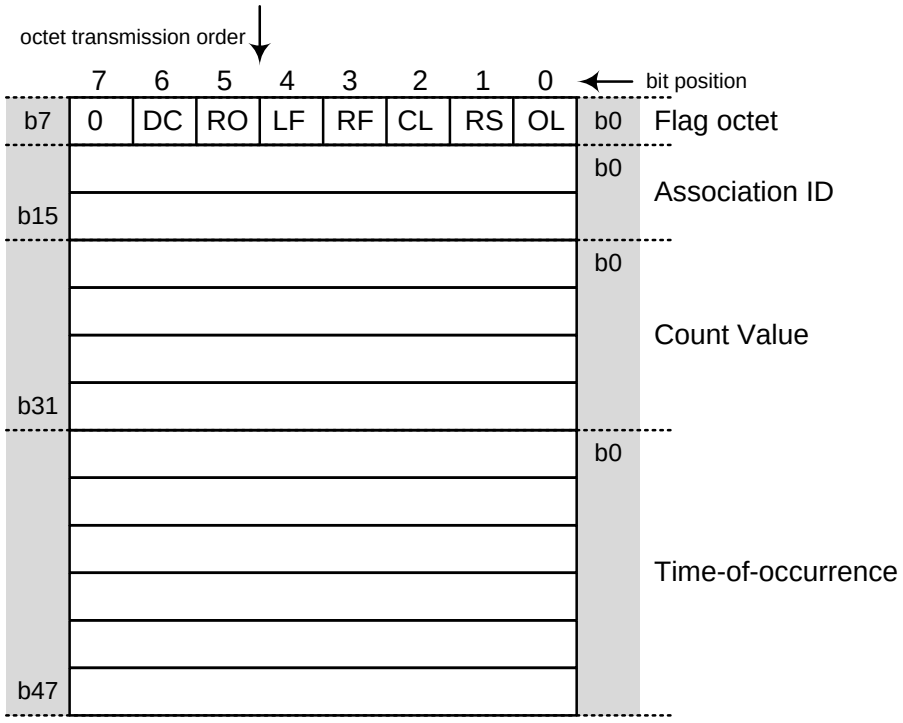
This object is used to report the value of a security statistic after the count has changed. See 11.5.6 for a description of a Security Statistic Point Type. Clause 11 specifies the point numbers permitted for this object and describes when the statistics are incremented.

Outstations shall not allow this object to be assigned to no class, or to static class 0.

Variation 2 objects contain a 32-bit, unsigned integer count value and a timestamp.

A.47.2.2 Coding

A.47.2.2.1 Pictorial



A.47.2.2.2 Formal structure

BSTR8: Flag Octet

Bit 0: ONLINE

Bit 1: RESTART

Bit 2: COMM_LOST

Bit 3: REMOTE_FORCED

Bit 4: LOCAL_FORCED

Bit 5: ROLLOVER

Bit 6: DISCONTINUITY

Bit 7: Reserved, always 0.

UINT16: Association ID

This value shall uniquely identify the association between the master and outstation on which the statistic is measured. The definition of a DNP association may be found in Clause 13. Because of the variety of configurations of DNP implementations, the Association ID may correspond to different combinations of DNP addresses, IP addresses, and port numbers or identifiers on the master and outstation. The Association ID shall be unique within the device. A value of 0 for Association ID means the statistic was measured on the same association on which this object is reported.

UINT32: Count value

This is the most recently obtained or computed value.

Range is 0 to +4294967295.

DNP3TIME: Time-of-occurrence

Time when the event occurred expressed in standard DNP time.

A.47.2.2.3 Notes

See 11.6 for flag bit descriptions.