IEC/TS 62351-5

Edition 2.0 2013-04

TECHNICAL SPECIFICATION

Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TS 62351-5

Edition 2.0 2013-04

TECHNICAL SPECIFICATION

Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-83220-732-1

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 5: Security for IEC 60870-5 and derivatives

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC/TS 62351-5, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This second edition cancels and replaces the first edition published in 2009. It constitutes a technical revision. The primary changes in the second edition are:

- adds the capability to change Update Keys remotely;
- adds security statistics to aid in detecting attacks;
- adds measures to avoid being forced to change session keys too often;
- discards unexpected messages more often as possible attacks;
- adds to the list of permitted security algorithms;
- adds new rules for calculating challenge sequence numbers.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/1204/DTS	57/1282/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Capitalization has been used in the text of this specification to formally identify the most important components of the described security mechanism. These components include: 1) data items e.g. Update Keys, Session Keys; 2) message names, e.g. Challenge, Reply, Aggressive Mode Request; 3) event names e.g. Reply Timeout, Rx Invalid Reply; 4) state names, e.g. Security Idle, Wait for Reply; and 5) statistics e.g. Authentication Failures, Unexpected Messages.

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 5: Security for IEC 60870-5 and derivatives

1 Scope and object

This part of IEC 62351 specifies messages, procedures and algorithms for securing the operation of all protocols based on or derived from IEC 60870-5: Telecontrol equipment and systems – Transmission protocols. This Technical Specification applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-102	Companion standard for the transmission of integrated totals in electric power systems
IEC 60870-5-103	Companion standard for the informative interface of protection equipment
IEC 60870-5-104	Network access for IEC 60870-5-101 using standard transport profiles
DNP3	Distributed Network Protocol (based on IEC 60870-1 through IEC 60870-5 and controlled by the DNP Users Group)

The initial audience for this Technical Specification is intended to be the members of the working groups developing the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

Portions of this specification may also be of use to managers and executives in order to understand the purpose and requirements of the work.

This part of IEC/TS 62351 focuses only on application layer authentication and security issues arising from such authentication. Other security concerns – in particular, protection from eavesdropping or man-in-the-middle attacks through the use of encryption – are considered to be outside the scope. Encryption may be added through the use of this specification with other specifications.

This document is organized working from the general to the specific, as follows:

- Clauses 2 through 4 provide background terms, definitions, and references.
- Clause 5 describes the problems this specification is intended to address.
- Clause 6 describes the mechanism generically without reference to a specific protocol.
- Clauses 7 and 8 describe the mechanism more precisely and are the primary normative part of this specification.
- Clause 9 describes a few particular implementation issues that are special cases.
- Clause 10 describes the requirements for other standards referencing this specification.

- Clause 11 describes the Protocol Implementation Conformance Statement (PICS) for this mechanism.

Unless specifically labelled as informative or optional, all clauses of this specification are normative.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Transmission protocols*

IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC/TS 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC/TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

ISO/IEC 9798-4, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*

ISO/IEC 11770-2:2008, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

FIPS 180-2, *Secure Hash Standard* (includes SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512). USA NIST

FIPS 186-2, *Digital Signature Standard (DSS),* USA NIST, February 2000 including Change Notice #1, October 2001. Used for the random number generation algorithms in the Appendix

FIPS 186-3, *Digital Signature Standard (DSS),* USA NIST, June 2009. Used for digital signature algorithms when asymmetric Update Key change is implemented

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*

RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

RFC 3629, *UTF-8, a transformation format of ISO 10646*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62351-2 and the following apply.

3.1
challenger
station that issues authentication challenges

Note 1 to entry: It may be either a controlled or controlling station.

3.2
control direction
direction of transmission from the controlling station to a controlled station

[SOURCE: IEC 60870-5-101:2003, 3.3]

3.3
controlled station
station which is monitored, or commanded and monitored by a master (controlling) station

Note 1 to entry: It is commonly called an “outstation” or “slave” in some specifications.

[SOURCE: IEC 60870-1-3:1997]

3.4
controlling station
station which performs the telecontrol of outstations

Note 1 to entry: It is commonly called a “master” or “master station” in some specifications.

[SOURCE: IEC 60870-1-3:1997]

3.5
monitor direction
direction of transmission from a controlled station to a controlling station

[SOURCE: IEC 60870-5-101:2003, 3.4]

3.6
responder
station that responds or reacts to authentication challenges

Note 1 to entry: It may be either a controlled or controlling station.

3.7
telecontrol
control of operational equipment at a distance using the transmission of information by telecommunication techniques

Note 1 to entry: Telecontrol may comprise any combination of command, alarm, indication, metering, protection and tripping facilities, without any use of speech messages.

[SOURCE: IEC 60870-1-3:1997]

3.8
application service data unit
ASDU
application layer message submitted to lower layers for transmission

4 Abbreviated terms

Refer to IEC/TS 62351-2 for a list of applicable abbreviated terms. The following term is included here because it is specifically used in the affected protocols and used in the discussion of this authentication mechanism.

ASDU	application service data unit. The application layer message submitted to lower layers for transmission.

5 Problem description (informative)

5.1 Overview of clause

Clause 5 describes:

- the security threats that this specification is intended to address;
- the unique design problems in implementing authentication for IEC 60870-5 and derived protocols;
- the resulting design principles behind the mechanism.

5.2 Specific threats addressed

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

- spoofing;
- modification;
- replay;
- eavesdropping – on exchanges of cryptographic keys only, not on other data.

5.3 Design issues

5.3.1 Overview of subclause

Subclause 5.3 describes the challenges faced in developing an authentication proposal that can be applied to all the IEC 60870-5 and derivative protocols. Subclause 5.3 is supplied for the benefit of security experts reviewing this document who may not be familiar with the electrical utility protocol environment.

5.3.2 Asymmetric communications

All the protocols affected by this specification share the concept of inequality between the communication stations. In each of these protocols there is a designated controlling station and a designated controlled station, each having different roles, responsibilities, procedures and message formats. In particular, the controlling station is in many cases responsible for flow control and media access control.

The existence of a definite controlled/controlling station designation has two impacts on the design of this authentication mechanism:

- the format of messages in each direction will differ, even if the functions are the same;
- key distribution is simplified because they will always be issued by the controlling station.

5.3.3 Message-oriented

All of the affected protocols are message-oriented. This means that authentication must be performed on a message-by-message basis, rather than authenticating only at the beginning of a data stream and occasionally thereafter, as some connection-oriented protocols do.

5.3.4 Poor sequence numbers or no sequence numbers

A common security technique to address the threat of replay is to include in the message a sequence number. Combined with tests for message integrity, the sequence number makes it harder for an attacker to simulate a legitimate user by just copying an existing message, because the messages must be transmitted in a particular order.

Unfortunately, none of the affected protocols includes a sequence number that would provide adequate protection. Those sequence numbers that do exist have very low maximum values, permitting an attacker to attempt a replay after gathering only a small number of messages.

Therefore, the design of this specification must include its own sequence numbers and other time-varying data to protect against replay.

5.3.5 Limited processing power

The lack of processing power available on many power utility devices has been a major design concern for the affected protocols since their creation. This design requirement necessarily affects the authentication mechanism also. The concern is heightened by the fact that many of these devices are single-processor machines; a denial-of-service attack would affect not only the communications capability of such devices but their function as an electrical control, protection, or monitoring device also.

Therefore, the use of security measures requiring extremely high processing power, such as public-key encryption and very large key sizes, has been avoided as much as possible.

5.3.6 Limited bandwidth

The limited amount of bandwidth available in utility networks has been the prime design concern (after message integrity) of the affected protocols. Links of 1 200 bits per second and lower are still a reality for many applications of these protocols. Some communications links also charge costs per octet transmitted.

Therefore the authentication mechanism must not add very much overhead (i.e. few octets) to the affected protocols. The size of the challenge and authentication data has therefore been limited and truncated as much as possible while retaining an adequate level of security. Other measures may be taken in the implementations in each protocol.

5.3.7 No access to authentication server

The nature of the utility networks in which the affected protocols are deployed is that the controlling station is often the only device with which the controlled station can communicate. If there is any access to other networks, it is often achieved through the device implementing the controlling station.

The impact of this fact on the authentication mechanism is that any system requiring on-line verification of the controlling station’s security credentials by a third party is not practical.

5.3.8 Limited frame length

Because of the restrictions on bandwidth and message integrity, the affected protocols are designed to send data in small frames of 255 octets or less. Some derivative protocols permit “chaining” frames together to create larger application layer messages.

However, in general, the authentication mechanism cannot assume the transmission of large data units between the stations.

5.3.9 Limited checksum

Message integrity was a high priority in the design of the affected protocols. However, the integrity measures chosen for these protocols were designed to protect against random noise, and not a concerted attack, as discussed below.

- The serial IEC 60870-5 protocols use Frame Type FT1.2, which uses parity bits and a single-octet checksum to protect against bit errors. A single octet is not large enough to provide a secure message authentication code (MAC).
- The IEC 60870-5-104 protocol depends on the integrity measures of lower layers. Because this specification discusses an application layer mechanism only, it cannot depend on such measures. In any case, doing so would provide a solution for only one of the affected protocols.
- The DNP3 protocol uses the IEC 60870-5 FT3 frame, with a two-octet cyclic redundancy check every 16 octets or fewer. This provides considerable integrity for security purposes, except that there is no check for the entire frame.

Therefore, the authentication mechanism described in this specification cannot make use of the existing protocol integrity mechanisms to provide message integrity for security purposes.

5.3.10 Radio systems

The affected protocols are often used over radio systems which may or may not provide security measures of their own. Many existing utility radio networks provide no security at all.

Therefore, the mechanism described in this specification must assume a hostile and physically insecure transmission environment.

5.3.11 Dial-up systems

The affected protocols are often used over dial-up telephone networks which require several seconds to re-establish communications before each frame transmitted. Similarly, many radio systems require long “keying” times before each frame.

Therefore, the authentication mechanism provides an option, known as “aggressive mode” that reduces the number of extra frames of data to be transmitted.

5.3.12 Variety of protocols affected

The IEC 60870-5 family of protocols share many common functions and an underlying design philosophy. However, the various companion standards and derivative protocols have been implemented using a variety of message formats and procedures.

Therefore, this specification describes a generic authentication mechanism that must be mapped to each specific affected protocol within specifications that are specific to that protocol.

5.3.13 Differing data link layers

As discussed in 5.3.9, the affected protocols use a variety of transport mechanisms and procedures. Although IEC 60870-5 describes a common data link layer, it permits multiple frame formats and other options. Several of the affected protocols use the FT1.2 frame, one uses FT3, and one does not use that frame format at all. Some of them use only an unbalanced media access control procedure, some use a balanced method, and some optionally use both.

Therefore, the authentication mechanism cannot be based on the data link layer. However, it can assume that there is addressing information available from lower layers that can be used for authentication.

5.3.14 Long upgrade intervals

Utilities depreciate changes to their networks over long periods, and may deploy several different generations of network systems simultaneously.

Therefore, this authentication mechanism follows the principles described in 5.4.8.

5.3.15 Remote sites

The devices that implement the affected protocols are often located at sites that are very remote and expensive to access.

Therefore, as much as possible, this mechanism includes methods of updating security credentials remotely.

5.3.16 Multiple users

A common topology for the affected protocols is for multiple users (such as control consoles, or operators) to access the controlled station through a single controlling station. For non-repudiation purposes, it is important to know which of these users sent a particular command of the controlled station.

Therefore, this mechanism includes methods to authenticate individual users separately from the controlling station itself.

5.3.17 Unreliable media

The affected protocols are often used over unreliable media. This mechanism attempts to take this unreliability into account when addressing error conditions. For instance, it does not assume that the loss of a single security message necessarily means that an attack is underway.

5.4 General principles

5.4.1 Overview of subclause

Subclause 5.4 describes the guiding principles behind this specification, based on the identified threats and design issues discussed in the previous two clauses.

5.4.2 Authentication only

As discussed Clause 1, this specification addresses authentication only, not encryption or other security measures. It does not rule out the possibility of such measures being added to the affected protocols by other standards.

5.4.3 Application layer only

This specification describes authentication at the application layer. Refer to IEC/TS 62351-1 for a discussion of why application layer authentication is necessary in the utility environment, in addition to any transport layer security that may be implemented.

5.4.4 Generic definition mapped onto different protocols

This specification describes a common method of authentication that can be used by any of the affected protocols. The implementation of this method in each protocol shall be defined by separate standards. Such standards shall reference this specification according to the rules defined in Clause 10.

5.4.5 Bi-directional

This specification describes a mechanism that can be used in either transmission direction, despite the asymmetry of communications traffic defined by the affected protocols and discussed in 5.3.2.

5.4.6 Challenge-response

The mechanism described in this specification is based on the concept of challenge and reply. 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 the affected protocols, the term used in this specification is “reply”.

5.4.7 Pre-shared keys as default option

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

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

5.4.8 Backwards tolerance

This specification 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 should be able to detect that the non-secure device does not support the authentication mechanism.
- The non-secure device should 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 should 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 protocol it is mapped to, and on the quality of the implementation on any particular device. This specification therefore recommends that secure devices avoid sending security messages if it is not known whether the remote device supports security. Remote configuration of security or non-security is beyond the scope of this document.

5.4.9 Upgradeable

This specification 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.

5.4.10 Perfect forward secrecy

This specification follows the security principle of perfect forward secrecy, as defined in IEC/TS 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.

5.4.11 Multiple users and auditing

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

The intent of this principle is to permit the controlled station to conclusively identify the individual user (not just the station) that transmits any protocol message. This information could be used to create an audit trail for security purposes. 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 addresses, and the affected user. For the best forensic results, stations 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 specification.

This specification allows for the possibility that controlled stations may limit access to certain functions, either based on the individual identities of users, or based on the “roles” the users perform. The User Number discussed in this document can be considered to represent not just a user, but a user acting in a particular role. This role-based access control (RBAC) is only possible if one of the optional methods for remotely changing pre-shared keys is implemented.

6 Theory of operation (informative)

6.1 Overview of clause

Clause 6 describes the operation of the authentication mechanism in general terms for the benefit of first-time readers. Clause 6 is informative only; in the case of disagreements between this clause and Clause 7, Clause 7 shall be taken as correct.

6.2 Narrative description

6.2.1 Basic concepts

The authentication mechanism is based on two concepts:

- A challenge and response protocol, as discussed in 5.4.6. The general mechanism is illustrated in Figure 2. Because “response” is a keyword in the affected protocols, the term used here is “reply”.

- The concept of a Message Authentication Code (MAC) that both the controlled and controlling stations calculate based on each Application Service Data Unit (ASDU, or protocol message) that is to be authenticated.

An 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-reply mechanism using an MAC is a “unilateral, two-pass authentication” mechanism as described in ISO/IEC 9798-4.

6.2.2 Initiating the challenge

The challenge may be initiated either by the controlling station or the controlled station. Since the IEC 60870-5 protocols are generally asymmetric, this means that the actual format of the challenge and reply messages will be somewhat different in the control and monitoring directions.

Stations 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.

Controlled stations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical. Other mandatory critical operations are described in 7.3.3.2. Each affected protocol 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 reply.

6.2.3 Replying to the challenge

The station (either controlling or controlled) that receives the challenge must respond 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 stations is an integral part of the computation. The following types of information are included in the computation:

- Some addressing information, specific to each protocol, is included in order to authenticate the responder as a valid application layer user.
- 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.

6.2.4 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.

6.2.5 Authentication failure

If the authentication fails, the challenger shall not use data from the challenged message. If the challenger is a controlled station, it shall not perform the operation requested by the controlling station. 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 8.2.5.3 for more details about the configurable maximum error count.

6.2.6 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 eliminates the challenge and reply messages.

Stations are required to implement Aggressive Mode, but shall provide a mode of operation in which it can be configured as disabled.

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 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.

6.2.7 Changing keys

6.2.7.1 General

Table 2 and Table 3 summarize how cryptographic keys are used and updated in this authentication mechanism. At a minimum, keys are managed by the controlled station and controlling station. Optionally, a trusted third party known as an authority may also help to manage the keys.

Table 2 – 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 controlled station.	The controlling station shall encrypt the Session Key in a Key Change message using the Update Key.	Minutes to weeks (for infrequent communications)
Control Direction Session Key	Used to authenticate data transmitted in the control direction by the controlling station.	The controlling station shall encrypt the Session Key in a Key Change message using the Update Key.	Minutes to weeks
Update Key	The controlling station shall use the Update Key to periodically change the Session Keys.	The Update Key may be pre-shared by the two stations, or if it is considered to be compromised, it may be changed remotely using either symmetric or asymmetric cryptography.	Months or years

Type	Use	Change mechanism	Range of expected change interval
Authority Certification Key (optional)	The authority shall use the Authority Certification Key to change Update Keys. The controlling station shall forward the Update Key encrypted by the authority to the controlled station.	The Authority Certification Key is pre-shared by the authority and the controlled station and can be changed only by means external to the protocol.	Years, if ever

Instead of using the Authority Certification Key, the authority, controlling station and controlled station 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 3 summarizes how these concepts may optionally be used to change Update Keys remotely.

Table 3 – 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 controlled station 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 controlled station by trusted personnel.	Years, if ever
User Private Key	The controlling station 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 controlling station in a physical token by the user. In any case, the mechanism by which the controlling station accesses the user’s private key must be secure.	Months or years
User Public Key	The controlled station 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.

Type	Use	Change mechanism	Range of expected change interval
Controlled Station Private Key	The controlled station shall use its Private Key to decrypt a new Update Key.	The Controlled Station Private Key shall be generated by the controlled station and stored securely on the controlled station.	Years if ever
Controlled Station Public Key	The controlling station shall use the Controlled Station's Public Key to encrypt a new Update Key for a user.	The Controlled Station Public Key shall be generated by the controlled station and may be transmitted anywhere in the clear, although it must be installed and stored securely in the controlling station by trusted personnel.	Years if ever

Further information on key management and derivation may be found in IEC 62351-9, currently in development.

6.2.7.2 Managing Session Keys

The Session Keys that each station 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 controlling station end, identified by a User Number.

The controlling station initializes the Session Keys immediately after communication 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 controlling station 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 controlling station 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 6 and Figure 7. Like the normal authentication mechanism, it is also based on challenge and reply:

- The controlling station sends a Key Status Request message, which contains no data but serves to initiate the process.
- The controlled station replies with a Key Status message containing the current status of the keys and some challenge data.
- The controlling station 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 controlled station to authenticate that the correct entity is attempting to change the Session keys.
- The controlled station 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 controlling station 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 8.2.3.

If either station determines that the communications 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 controlling station shall send a Key Status Request at the earliest opportunity after detecting the communications failure, and re-initialize the Session Keys.

6.2.7.3 Managing Update Keys

As discussed in 5.4.11, this authentication mechanism permits multiple users of the system to be authenticated separately from the controlling station itself. Each user is identified by its own User Number and has its 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 specification, 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 controlling station 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 controlling station and controlled station 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 the affected protocol 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 1. 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 controlling station or controlled station shall be trusted with the capability to add or remove users from a controlled station, 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 1, the controlling station's job is merely to forward certifications of users to the controlled station from the authority, and to ensure that the new Update Key is securely transmitted. The communications between the controlling station and the authority for the purpose of certifying a user is out of the scope of this document but must also be secure.

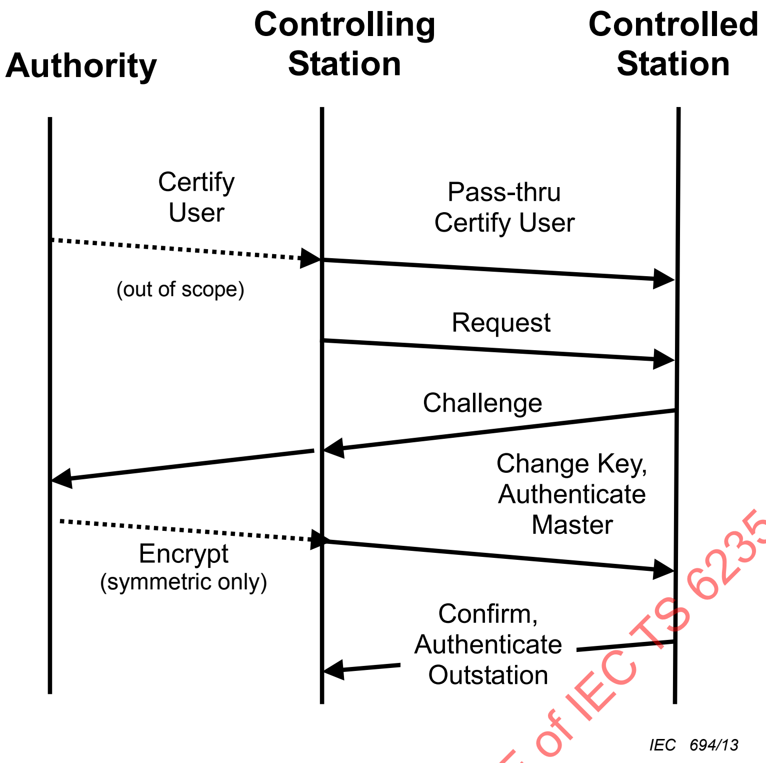

Figure 1 – Overview of interaction between Authority and stations

6.2.8 Security statistics

An important feature of the secure authentication mechanism is that it provides ability for the operators of the network to detect some kinds of attacks. Any controlled station implementing secure authentication must keep statistics on the operation of the protocol state machines and report those statistics as part of the normal operation of the affected protocol. If some statistics, e.g. authentication failures, begin to frequently exceed event reporting thresholds, it may indicate that an attack is underway. Controlled stations may report security statistics to controlling stations other than those involved in the authentication. This permits the operators of the network to detect attacks that may be occurring on other links than the one they are currently monitoring.

6.3 Example message sequences

6.3.1 Overview of subclause

Subclause 6.3 contains diagrams illustrating examples of how the authentication mechanism shall behave. Subclause 6.3 is informative only. Refer to Clause 7 for a formal description of the mechanism. Bold arrows in these diagrams represent authentication-specific messages.

6.3.2 Challenge of a Critical ASDU

Figure 2 and Figure 3 illustrate the challenge and reply to a Critical ASDU.

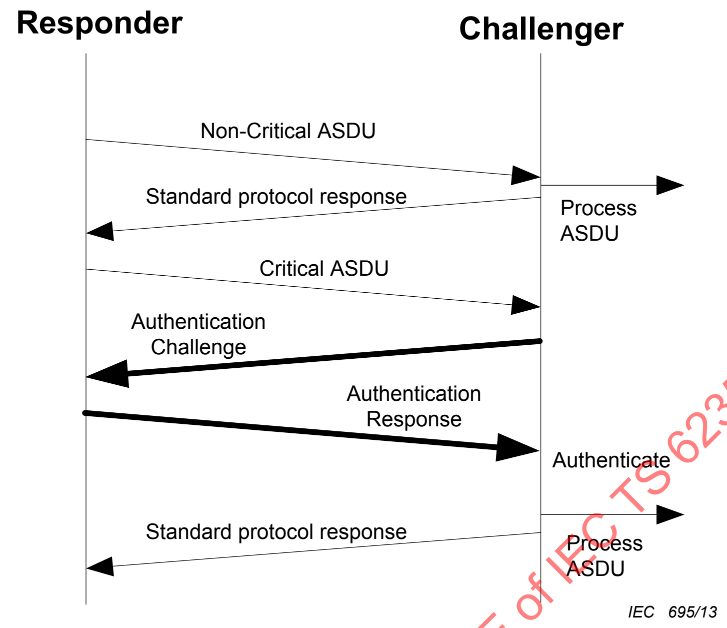

Figure 2 – Example of successful Challenge of Critical ASDU

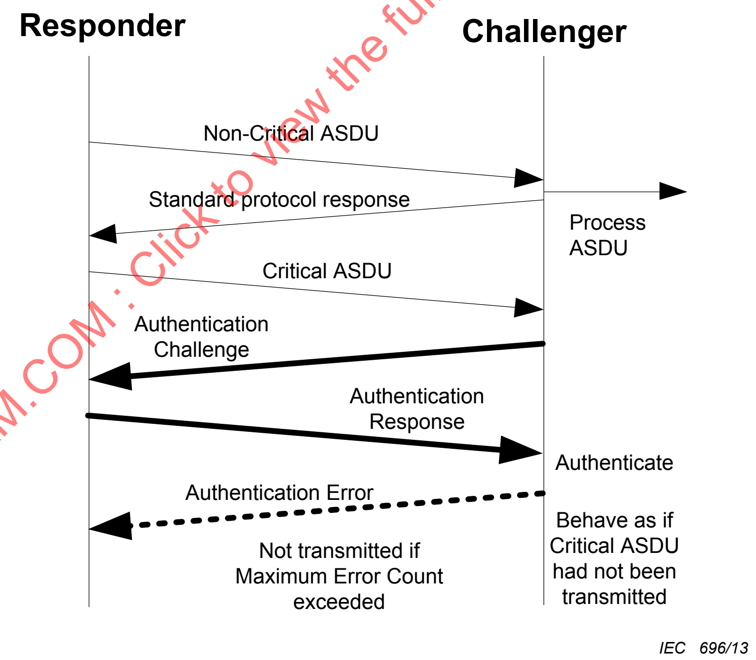

Figure 3 – Example of failed Challenge of Critical ASDU

6.3.3 Aggressive Mode

Figure 4 and Figure 5 illustrate authentication of a Critical ASDU using Aggressive Mode.

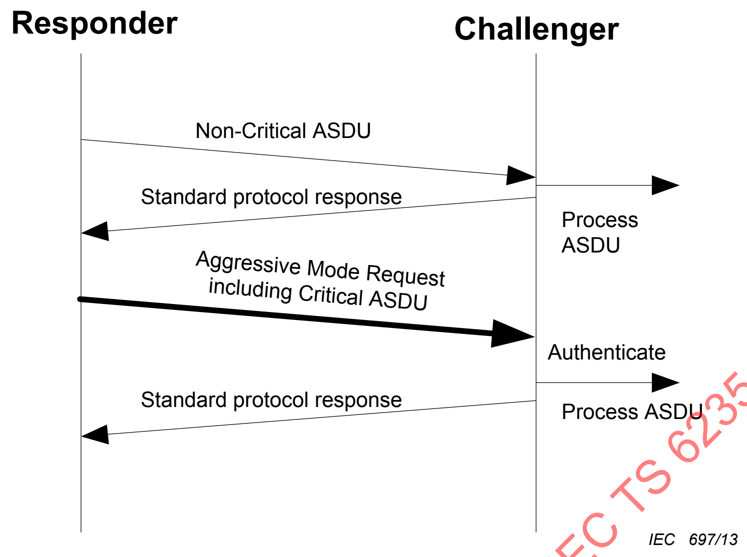
Responder
Challenger
Non-Critical ASDU
Standard protocol response
Process ASDU
Aggressive Mode Request including Critical ASDU
Authenticate
Standard protocol response
Process ASDU
IEC 697/13

Figure 4 – Example of a successful Aggressive Mode Request

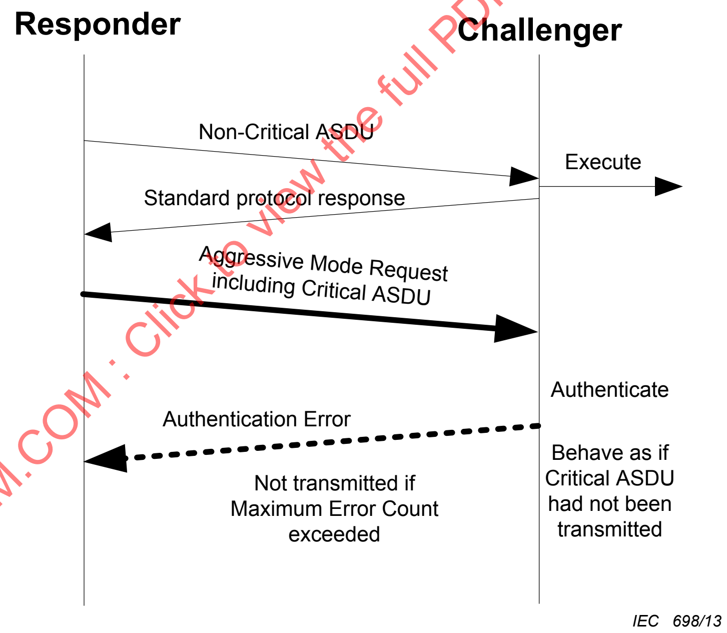
Responder
Challenger
Non-Critical ASDU
Execute
Standard protocol response
Aggressive Mode Request including Critical ASDU
Authenticate
Authentication Error
Behave as if Critical ASDU had not been transmitted
Not transmitted if Maximum Error Count exceeded
IEC 698/13

Figure 5 – Example of a failed Aggressive Mode Request

6.3.4 Initializing and changing Session Keys

Figure 6 and Figure 7 illustrate how the controlling station initializes and changes the Session Keys on startup, periodically, and after a communications failure. Figure 8 illustrates how the authority and controlling station may change a user's role (e.g. add the user or change the user's access permissions) and initialize or change the user's Update Key. Figure 9 illustrates how a user may change masters and continue communications with a controlled station 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 specification.

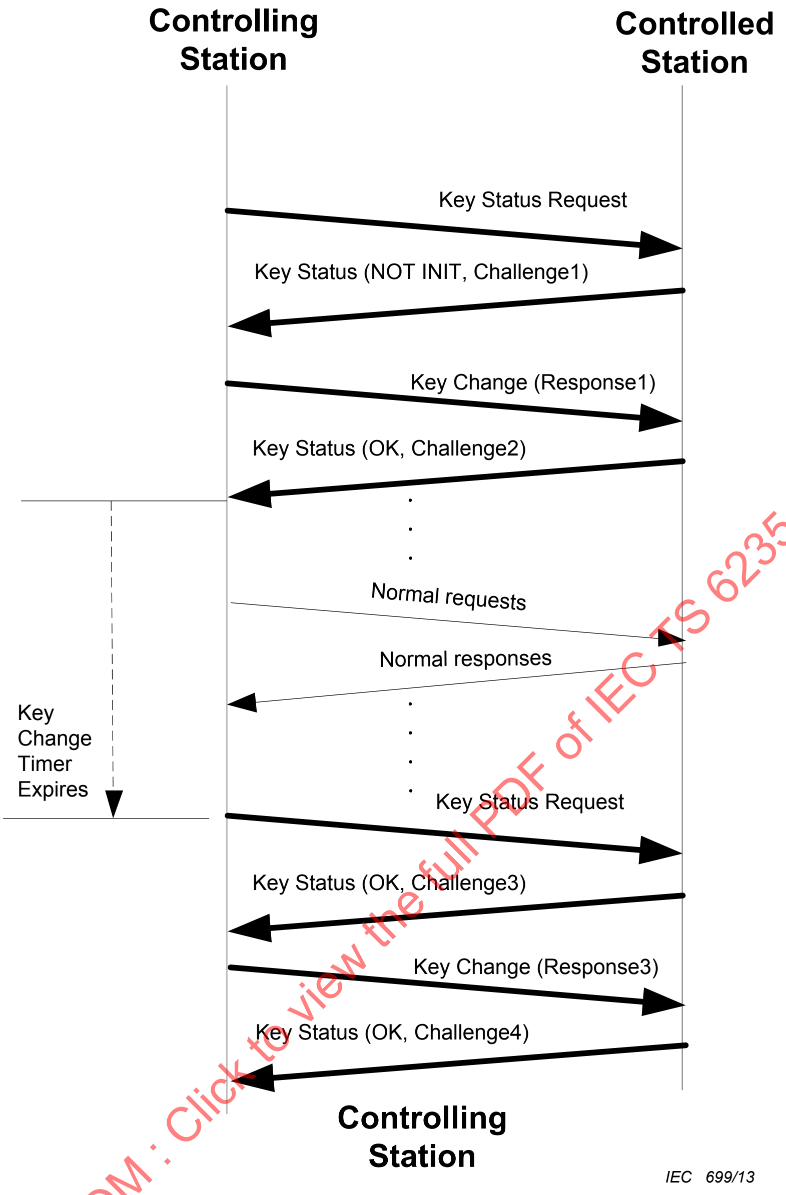

Figure 6 – Example of Session Key initialization and periodic update

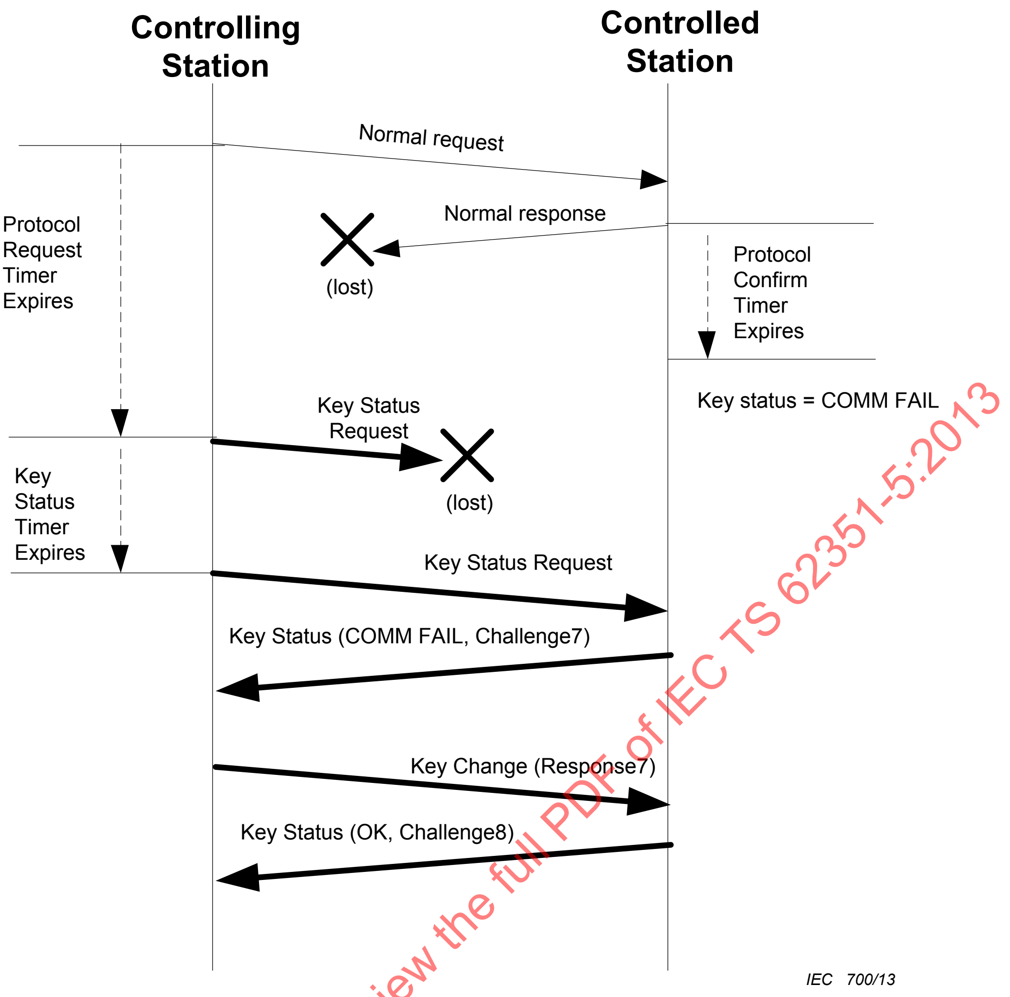

Figure 7 – Example of communications failure followed by Session Key change

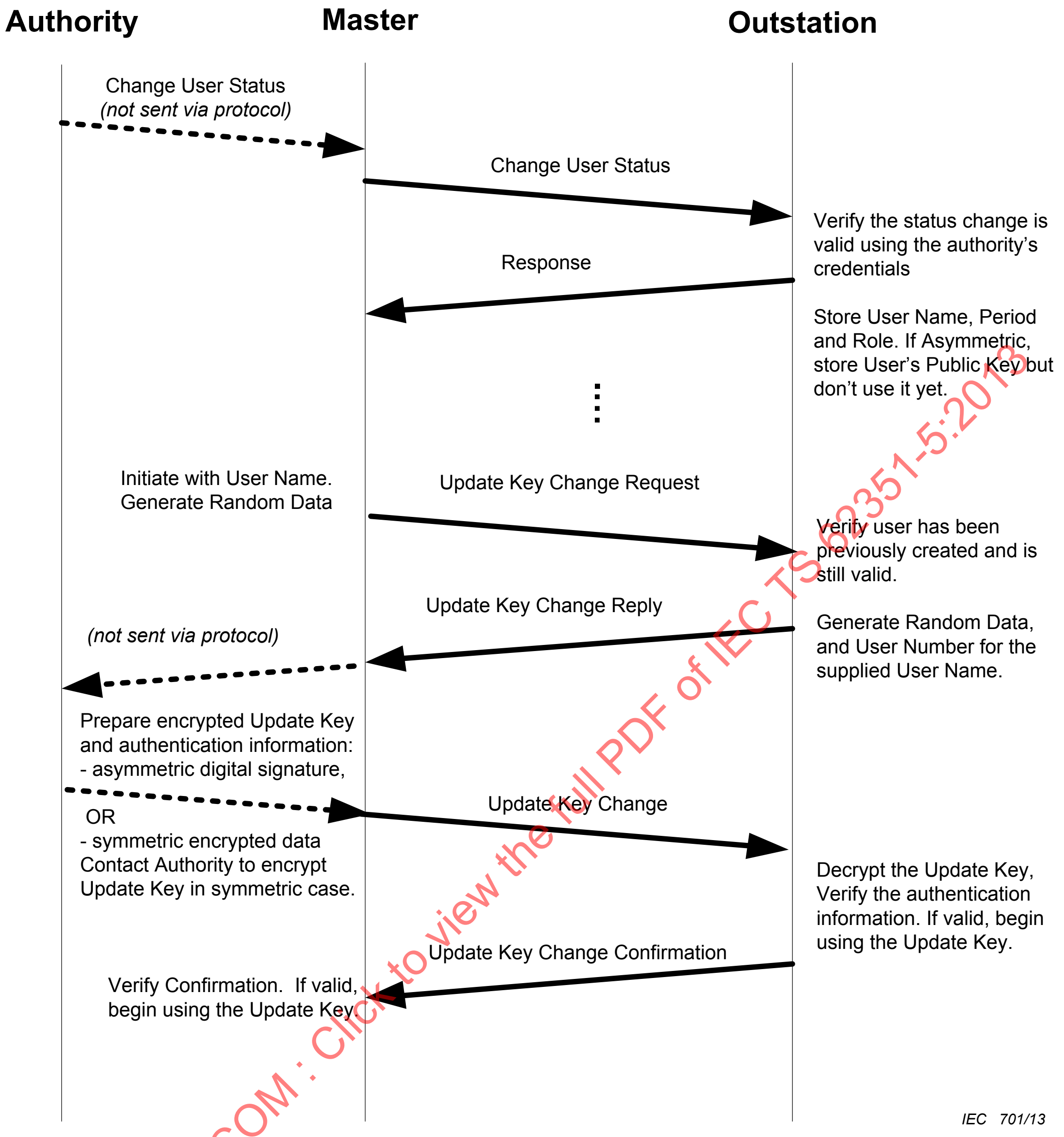
Authority
Master
Outstation
Change User Status
(not sent via protocol)
Change User Status
Verify the status change is valid using the authority's credentials
Response
Store User Name, Period and Role. If Asymmetric, store User's Public Key but don't use it yet.
Initiate with User Name. Generate Random Data
Update Key Change Request
Verify user has been previously created and is still valid.
Update Key Change Reply
(not sent via protocol)
Generate Random Data, and User Number for the supplied User Name.
Prepare encrypted Update Key and authentication information:
- asymmetric digital signature,
OR
- symmetric encrypted data
Contact Authority to encrypt Update Key in symmetric case.
Update Key Change
Decrypt the Update Key, Verify the authentication information. If valid, begin using the Update Key.
Update Key Change Confirmation
Verify Confirmation. If valid, begin using the Update Key.
IEC 701/13

Figure 8 – Example of successful User Status and Update Key Change

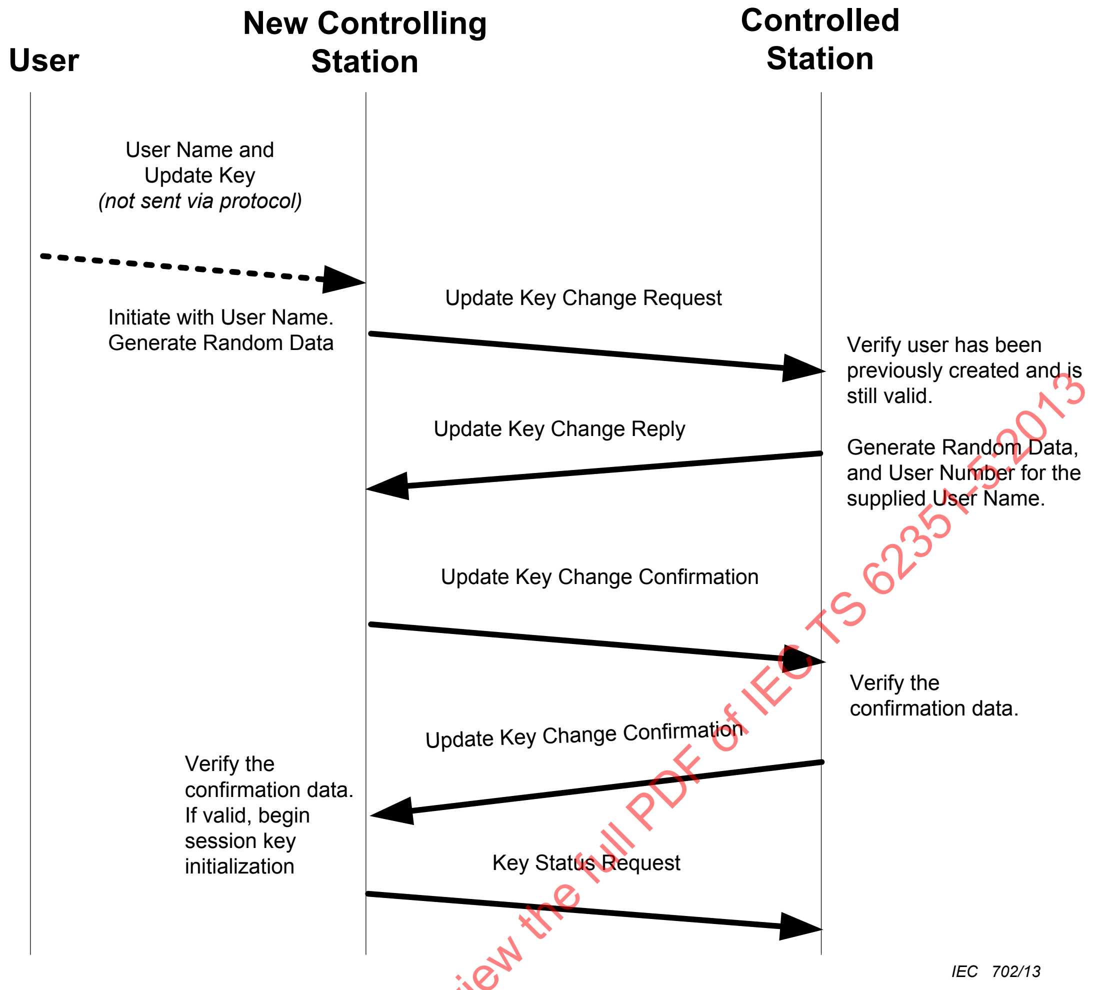
User
New Controlling Station
Controlled Station
User Name and Update Key (not sent via protocol)
Initiate with User Name. Generate Random Data
Update Key Change Request
Verify user has been previously created and is still valid.
Update Key Change Reply
Generate Random Data, and User Number for the supplied User Name.
Update Key Change Confirmation
Verify the confirmation data.
Update Key Change Confirmation
Verify the confirmation data. If valid, begin session key initialization
Key Status Request
IEC 702/13

Figure 9 – User changes controlling stations

6.4 State machine overview

Figure 10 and Figure 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. Figure 12 and Figure 13 illustrate the state machines for the controlling and controlled stations respectively, when changing the status, role or Update Key of a user.

The details of the state machines are specified in Clause 7. If these diagrams differ from Clause 7, that clause shall be considered to be correct.

The *Security Idle* and *Wait for Reply* states are common to both controlling and controlled stations. The other states are specific to each type of station.

For simplicity, these figures show a transition to the *Wait for Reply* state upon receiving an Aggressive Mode Request. In reality, as described in Table 30, this transition would be only momentary and the station would immediately return to *Security Idle* state after taking the appropriate action.

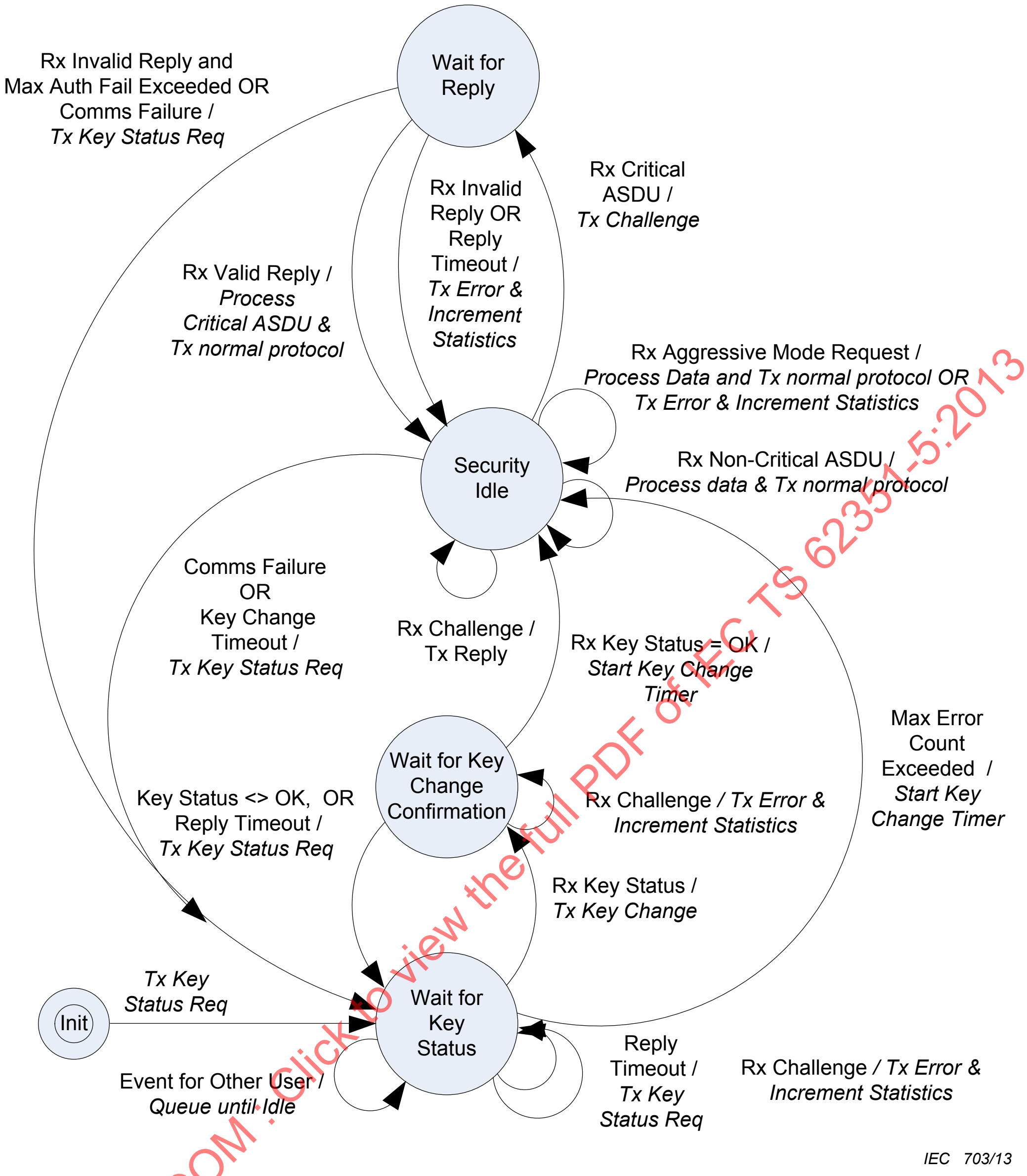
Wait for Reply
Rx Invalid Reply and Max Auth Fail Exceeded OR Comms Failure / *Tx Key Status Req*
Rx Invalid Reply OR Reply Timeout / *Tx Error & Increment Statistics*
Rx Critical ASDU / *Tx Challenge*
Rx Valid Reply / *Process Critical ASDU & Tx normal protocol*
Rx Aggressive Mode Request / *Process Data and Tx normal protocol OR Tx Error & Increment Statistics*
Security Idle
Rx Non-Critical ASDU / *Process data & Tx normal protocol*
Comms Failure OR Key Change Timeout / *Tx Key Status Req*
Rx Challenge / Tx Reply
Rx Key Status = OK / *Start Key Change Timer*
Max Error Count Exceeded / *Start Key Change Timer*
Wait for Key Change Confirmation
Key Status <> OK, OR Reply Timeout / *Tx Key Status Req*
Rx Challenge / *Tx Error & Increment Statistics*
Rx Key Status / *Tx Key Change*
Init
Tx Key Status Req
Wait for Key Status
Event for Other User / *Queue until Idle*
Reply Timeout / *Tx Key Status Req*
Rx Challenge / *Tx Error & Increment Statistics*
IEC 703/13

Figure 10 – Major state transitions for controlling station authentication

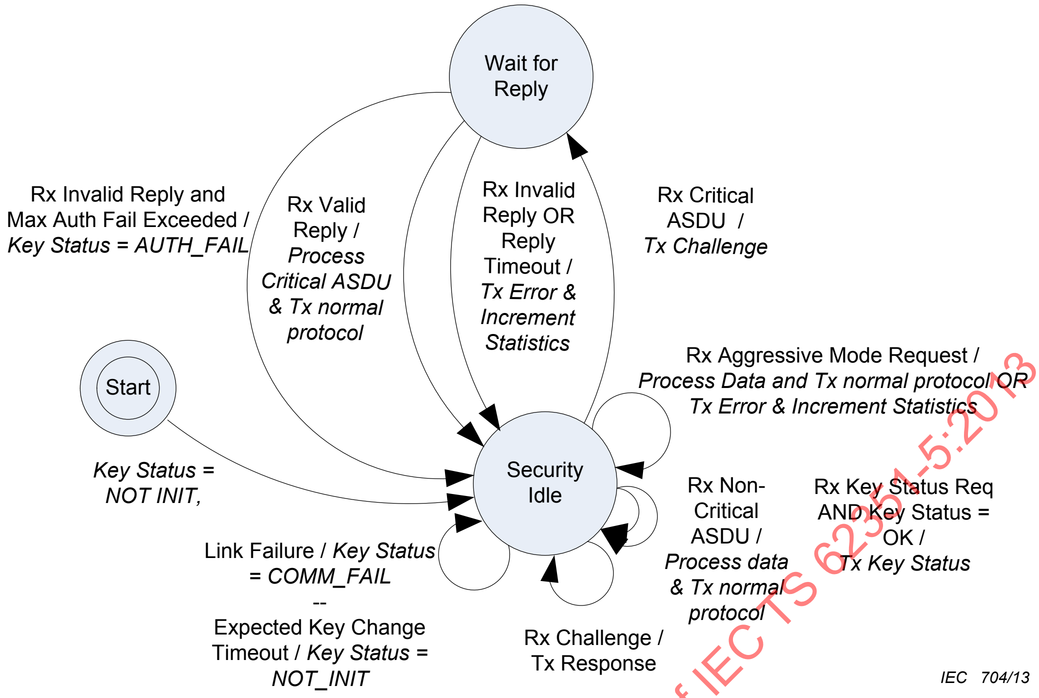
Wait for Reply
Rx Invalid Reply and Max Auth Fail Exceeded / Key Status = AUTH_FAIL
Rx Valid Reply / Process Critical ASDU & Tx normal protocol
Rx Invalid Reply OR Reply Timeout / Tx Error & Increment Statistics
Rx Critical ASDU / Tx Challenge
Rx Aggressive Mode Request / Process Data and Tx normal protocol OR Tx Error & Increment Statistics
Start
Security Idle
Key Status = NOT INIT,
Rx Non-Critical ASDU / Process data & Tx normal protocol
Rx Key Status Req AND Key Status = OK / Tx Key Status
Link Failure / Key Status = COMM_FAIL
--
Expected Key Change Timeout / Key Status = NOT_INIT
Rx Challenge / Tx Response
IEC 704/13

Figure 11 – Major state transitions for controlled station authentication

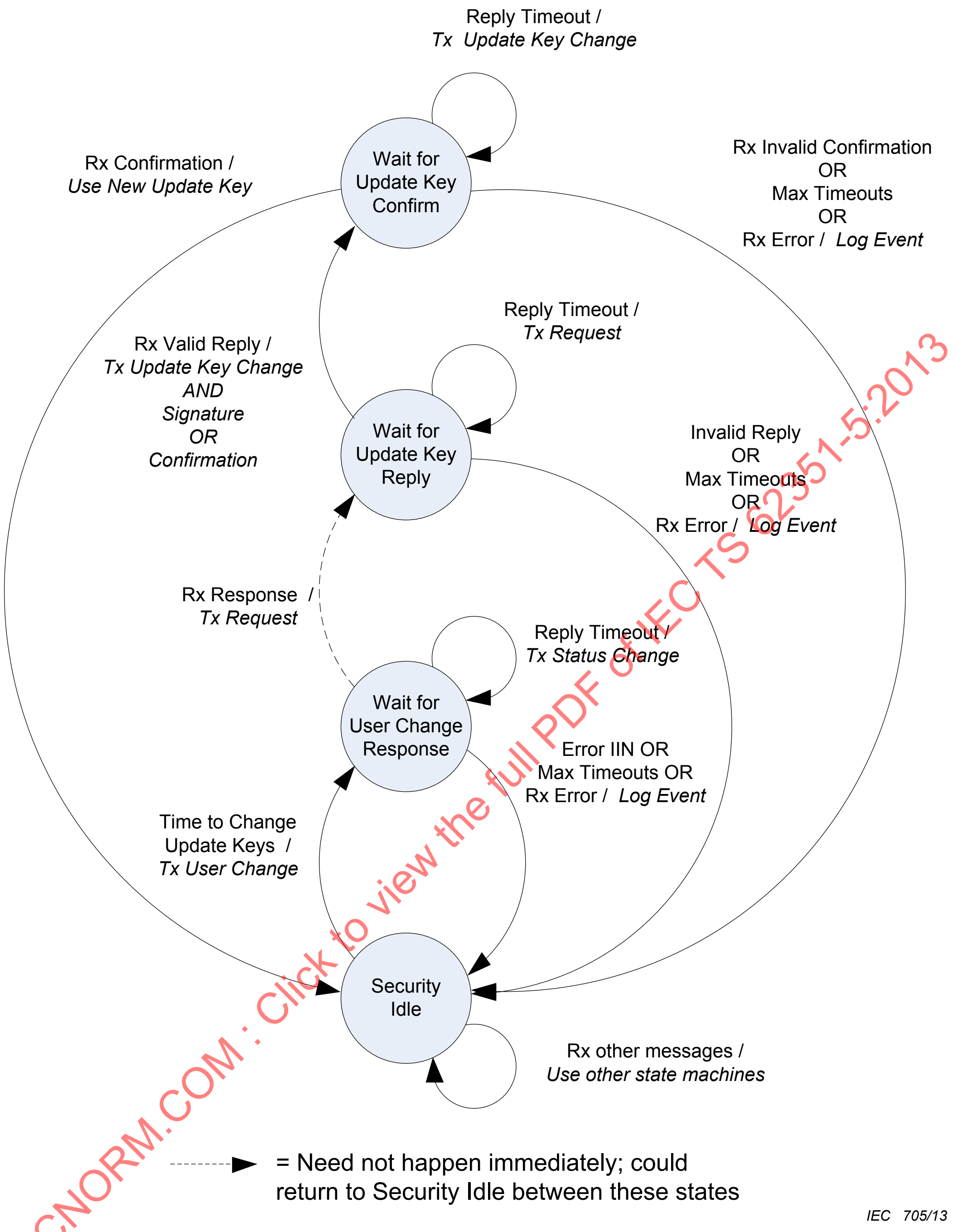

Figure 12 – Major state transitions for controlling station Update Key change

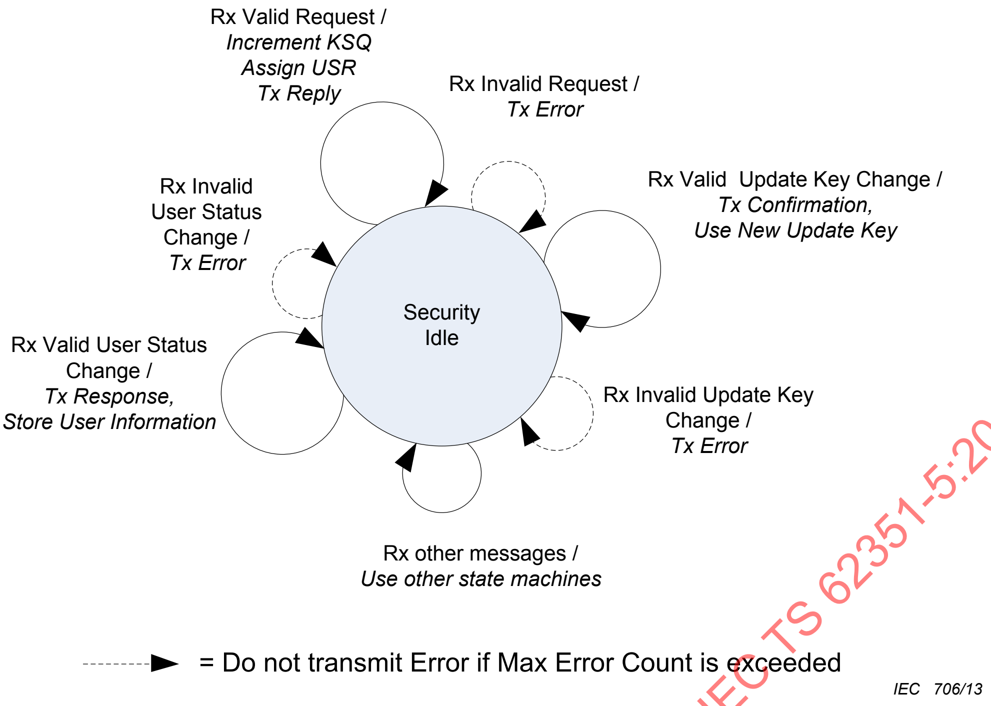

Figure 13 – Major state transitions for controlled station Update Key change

7 Formal specification

7.1 Overview of clause

Clause 7 formally describes the protocol used for this authentication mechanism. If Clause 7 differs from Clause 6, it shall be considered to be definitive.

7.2 Message definitions

7.2.1 Distinction between messages and ASDUs

Subclause 7.2 describes the data in each security message. A security message is not a complete ASDU. The list of data and the format of this data shall remain the same between protocols, but the ASDUs surrounding the message and the mechanisms used to deliver them shall differ per protocol. This mapping to the affected protocol shall be described in the specification for the affected protocol, as discussed in Clause 10. Note that all of the affected protocols transmit integer values with the least significant octet transmitted first; therefore that same convention shall be used for all the security messages.

7.2.2 Challenge message

7.2.2.1 Structure

Each Challenge message shall contain the information described in 7.2.2 and summarized in Table 4. A Challenge message shall be a request that the Responder authenticate itself to the Challenger.

Table 4 – Challenge message

Value	CSQ = Challenge sequence number, defined in 7.2.2.2
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.2.3
Value	
Enumerated value	MAL = MAC algorithm, defined in 7.2.2.4
Enumerated value	RSC = Reason for challenge, defined in 7.2.2.5
Value	CLN = Challenge data length, defined in 7.2.2.6
Value	
Number of octets specified in CLN	CHD = Pseudo-random challenge data, defined in 7.2.2.7

7.2.2.2 Challenge Sequence Number

Stations shall use this value to match replies with challenges as described in 7.3.3.3.

CSQ := UI32[1..32]<0.. 4294967295>

7.2.2.3 User Number

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

USR := UI16[1..8]<0..65535>

<0> := Unknown. The challenge-reply sequence is being initiated by a controlled station. Therefore the appropriate USR is not yet known. The controlling station will supply the appropriate USR in the Reply message.

<1> := Default: The challenge-reply sequence is being initiated by a controlling station on behalf of more than one user. The set of Session Keys used will therefore be the default set of keys for this pair of stations. Refer to 7.2.5.2 for more details.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

7.2.2.4 MAC Algorithm

Using this value, the Challenger shall specify the algorithm that the Responder shall use to calculate the MAC Value, as described in 7.2.3.5, and shall also specify the resulting length of the MAC Value, as described in 7.2.3.4. Refer to the normative references listed in Clause 2 for details of these algorithms. Each station shall support at least the minimum subset of algorithms listed in 8.2.2.

MAL := UI8[1..8]<0..255>

<0> := reserved

<1> := reserved

<2> := reserved

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

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

<5> := reserved

<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 the note in 8.2.5.3 regarding the dependency between the use of truncated MAC algorithms and the need for frequent Session Key changes. In any case, the longest practical MAC should be used whenever possible.

7.2.2.5 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.

RSC := UI8[1..8]<0..255>

<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

7.2.2.6 Challenge Data Length

This value shall specify the length in octets of the challenge data that follows. The minimum length of the challenge data shall be four octets.

CLN := UI16[1..16]<4..65535>

7.2.2.7 Pseudo-random Challenge Data

Stations 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 the FIPS 186-2 Digital Signature Standard.

CHD := OS8i[1..8i]; i:=CLN

7.2.3 Reply message

7.2.3.1 Structure

Each Reply message shall contain the information described in 7.2.3 and summarized in Table 5. A Reply message shall be a reply to a Challenge message.

Table 5 – Reply message

Value	CSQ = Challenge sequence number, defined in 7.2.3.2
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.3.3
Value	
Value	HLN = MAC length, defined in 7.2.3.4
Value	
Number of octets specified in HLN	MAC value, defined in 7.2.3.5

7.2.3.2 Challenge Sequence Number

This value shall be as described in 7.2.2.2. The value transmitted by the Responder in the Reply message shall be the same value transmitted by the Challenger in the previous Challenge message.

CSQ := UI32[1..32]<0.. 4294967295>

7.2.3.3 User Number

The controlling station shall use this value to identify which set of Session Keys is to be used to authenticate this Reply. If the Responder is the controlled station, this value shall be the same as the USR value transmitted by the Challenger in the previous Challenge message. If the Responder is the controlling station, it shall set the USR value according to which user is being authenticated. Refer to 7.2.5.2 for more details.

USR := UI16[1..16]<0..65535>

7.2.3.4 MAC Length

HLN := UI16[1..16]<2..65535>

The MAC Length shall specify the length of the MAC Value in octets. The MAC Length shall be correct for the MAC algorithm specified by the Challenger, as described in 7.2.2.4.

7.2.3.5 MAC Value

The Responder shall calculate the MAC Value according to the MAC algorithm specified by the Challenger, as described in 7.2.2.4. The Responder shall include in the MAC Value calculation the data listed in Table 6, in the order listed.

Table 6 – Data Included in the MAC Value calculation

Data	Description	Described in	Included
Challenge message	The entire Challenge message transmitted by the Challenger.	Subclause 7.2.2	Always.
Addressing information	Addressing information identifying the Challenger and Responder, specific to the protocol and found in the lower layers of the protocol.	Protocol specification	Always.
Challenged ASDU	The entire previous ASDU transmitted by the Responder, not including data link layer or APCI information.	Protocol specification	If the Reason For Challenging is <1>, challenging a critical function.
Padding Data	Any padding data required.	Hash specification	As required by the MAC algorithm.

Controlled stations acting as the Responder shall use the current Monitoring Direction Session Key to calculate the MAC Value.

Controlling stations acting as the Responder shall use the current Control Direction Session Key to calculate the MAC value.

MAC := OS8i[1..8i]; i:=HLN

7.2.4 Aggressive Mode Request message

7.2.4.1 Structure

In Aggressive Mode, a station shall supply authentication information in the same ASDU as the data it is authenticating. Aggressive Mode shall be mandatory, but can be disabled by configuration. Aggressive Mode is slightly less secure than normal mode operation, but uses considerably less bandwidth, especially if many critical functions must be authenticated.

Each Aggressive Mode Request message shall contain the information described in 7.2.4 and summarized in Table 7.

Table 7 – Aggressive Mode Request message

Value	CSQ = Challenge sequence number, defined in 7.2.4.3.
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.4.4
Value	
Number of octets specified in MAL	MAC value, defined in 7.2.4.5.

7.2.4.2 Aggressive Mode must be preceded by Challenge/Reply

The Responder shall not transmit an Aggressive Mode Request until the Responder has received and responded to at least one Challenge message from the Challenger. Refer to the procedures in 7.3.4 for more details.

The Responder shall use the data from the most recently received Challenge message to calculate the Challenge Sequence Number and MAC Value in the Aggressive Mode Request, as described in 7.2.4.3 and 7.2.4.5.

7.2.4.3 Challenge Sequence Number

The Challenge Sequence Number (CSQ) shall have the value described in 7.3.3.3. The effect of the rules described in that clause is that the CSQ of a given Aggressive Mode Request shall be the CSQ from the most recently received Challenge message, plus the number of Aggressive Mode Requests or Reply messages the Responder has transmitted since receiving that Challenge message.

7.2.4.4 User Number

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

USR := UI6[1..16]<0..65535>

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

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

- This message is being sent by a controlling station on behalf of more than one user.
- This message is being sent by a controlled station and there is no corresponding user.

In either case, the set of Session Keys used will be the default set for this pair of stations. Refer to 7.2.5.2 for more details.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

7.2.4.5 MAC 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 8 describes this difference.

Table 8 – Data Included in the MAC Value calculation in Aggressive Mode

Data	Description	Described in	Included
Challenge message	All the data from the most recently received Challenge message, including the CSQ at the time of that message.	Subclause 7.2.2	Always.
Addressing information	Addressing information identifying the Challenger and Responder, specific to the protocol and found in the lower layers of the protocol.	Protocol specification	Always.
Authenticated Data	The entire ASDU transmitted by the Responder, not including data link layer or APCI information.	Protocol specification	Always.
Padding Data	Any padding data required.	Hash specification	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 Responder, as described in 7.2.2.4.

Controlled stations acting as the Responder shall use the current Monitoring Direction Session Key to calculate the MAC Value.

Controlling stations acting as the Responder shall use the current Control Direction Session Key to calculate the MAC value.

7.2.5 MAC :=OS8i[1..8i]; i:=specified by MALKey Status Request message

7.2.5.1 General

Each Key Status Request message shall contain the information described in 7.2.5 and summarized in Table 9.

Only the controlling station shall send Key Status Request messages. The Key Status Request message shall elicit a Key Status message from the controlled station.

Table 9 – Key Status Request Message

Value	USR = User Number, defined in 7.2.4.4
Value	

7.2.5.2 User Number

The controlling station uses this value to identify the set of Session Keys for which it is requesting the current status.

USR := UI16[1..16]<0..65535>

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

<1> := Default. The default set of Session Keys used by this pair of stations, to be used as illustrated in Table 10.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

Table 10 – Use of Default Session Keys

Case	User Number
Controlled station sends Challenge	Unknown <0>
Controlled station sends Aggressive Mode Request	Default <1>
Controlling station challenges response or spontaneous data from controlled station	Default <1>
Controlling station sends request for data to be processed by multiple users	Default <1>
Any other case	<2..65535>

7.2.6 Key Status message

7.2.6.1 Structure

Each Key Status message shall contain the information described in 7.2.6 and summarized in Table 11.

Only the controlled station shall send Key Status messages. A Key Status message shall indicate to the controlling station the current status of the Session Keys and provide challenge data that the controlling station must use to authenticate itself when sending the next Key Change message.

If the Key Status = OK, meaning that the controlled station considers the Session Keys to be valid, the Key Status message is authenticated with an MAC.

Table 11 – Key Status Message

Value	KSQ = Key change sequence number, defined in 7.2.6.2
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.6.3
Value	
Enumerated value	KWA = Key wrap algorithm, defined in 7.2.6.4
Enumerated value	KST = Key status, defined in 7.2.6.5
Enumerated value	MAL = MAC algorithm, defined in 7.2.6.6
Value	KCL = Key Status challenge data length, defined in 7.2.6.7
Value	
Number of octets specified in KCL	KCD = Key status pseudo-random challenge data, defined in 7.2.6.8
Number of octets specified in MAL	MAC value, defined in 7.2.6.9

7.2.6.2 Key Change Sequence Number

Each controlled station 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 initialised to zero on start-up of the controlled station (unless the MAC algorithm is AES-GMAC; refer to 8.3.2.1). The controlled station shall increment the KSQ each time it receives a Key Change or Key Status Request message. (The first KSQ transmitted shall therefore always be 1). If the value reaches 4294967295, the next KSQ the controlled station transmits shall be zero.

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

KSQ := UI32[1..32]<0.. 4294967295>

7.2.6.3 User Number

The controlled station 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 Key Status Request message, as described in 7.2.5.2.

7.2.6.4 Key Wrap Algorithm

Using this value, the controlled station shall indicate to the controlling station the algorithm it will use to decrypt the data in subsequent Key Change messages. Refer to the normative references listed in Clause 2 for details of these algorithms. Each station shall support at least the minimum subset of algorithms listed in 8.2.3.

KWA := UI8[1..8]<0..255>

<0> := not used

<1> := AES-128 Key Wrap Algorithm, as described in 8.2.3.2.

<2> := AES-256 Key Wrap Algorithm, as described in 8.3.4.1

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

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

7.2.6.5 Key Status

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

KST := UI8[1..8]<0..255>

<0> := not used

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

<2> := NOT INIT. The controlled station has not received an authentic Key Change message since it last started up. The Session Keys are not valid.

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

<4> := AUTH FAIL. The controlled station has received a non-authentic Challenge or Aggressive Mode Request. The Session Keys are not valid.

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

7.2.6.6 MAC Algorithm

Using this value, the controlled station shall specify the algorithm that the controlling station shall use to calculate the MAC Value in this message, as described in 7.2.6.9, and shall also specify the resulting length of the MAC Value.

The enumerated values used to specify the MAC algorithm are defined in 7.2.2.4, except for the following:

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

7.2.6.7 Key Status challenge data length

This value shall specify the length in octets of the challenge data that follows. The minimum length of the challenge data shall be eight octets.

KCL := UI16[1..16]<8..65535>

7.2.6.8 Key Status pseudo-random challenge data

The controlled station shall include this pseudo-random data in the Key Status message to ensure that the contents of the Key Status message are not predictable. The pseudo-random data shall be generated using the algorithm specified in the *FIPS 186-2 Digital Signature Standard*.

KCD := OS8i[1..8i]; i:=CLN

7.2.6.9 MAC Value

The controlled station shall calculate the MAC Value according to the MAC algorithm MAL, as described in 7.2.6.6. The controlled station shall include in the MAC Value calculation the data listed in Table 12, in the order listed. It shall use the Monitoring Direction Session Key from the Key Change message most recently received from the controlling station.

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 message.

Table 12 – Data Included in the MAC Value Calculation for Key Status

Data	Description	Included
Challenge message	The entire ASDU containing the Key Change message most recently received by the controlled station.	Always.
Padding Data	Any padding data required.	As required by the MAC algorithm.

MAC := OS8i[1..8i]; i:=as specified in MAL

7.2.7 Session Key Change message

7.2.7.1 Structure

Each Key Change message shall contain the information described in 7.2.7 and summarized in Table 13. A Key Change message shall be a notice from the controlling station of a change in the Session Keys.

Table 13 – Key Change message

Value	KSQ = Key Change sequence number, defined in 7.2.7.2
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.7.3
Value	
Value	WKL = Wrapped key data length, defined in 7.2.7.4
Value	
Number of octets specified in WKL	WKD = Wrapped key data, defined in 7.2.7.5

7.2.7.2 Key Change Sequence Number

This value shall match the KSQ transmitted in the Key Status message most recently received by the controlling station, as described in 7.2.6.2.

KSQ := UI32[1..32]<0.. 4294967295>

7.2.7.3 User Number

The controlling station shall use this value to specify which set of Session Keys is to be changed. It shall match the USR in the Key Status message most recently received by the controlling station, as described in 7.2.6.3.

7.2.7.4 Wrapped Key Data Length

This value shall be the length of the data produced by the Key Wrap algorithm, as described in 7.2.7.5.

WKL := UI16[1..16]<8 ..65535>

7.2.7.5 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 controlling station shall pass the data through the Key Wrap Algorithm in the order described in Table 14.

Table 14 – Data Included in the key wrap (in order)

Data	Description	Described in	Included
Session Key Length	The size of one of the Session Keys. Both keys are the same length. This value is two octets long.	Subclause 8.2.4.2	Always
Control Direction Session Key	The key used to authenticate data from the controlling station.	Subclause 7.2.3.5 and 7.2.4.5	Always
Monitoring Direction Session Key	The key used to authenticate data from the controlled station.	Subclause 7.2.3.5 and 7.2.4.5	Always
Key Status message	All data in the Key Status message most recently received from the controlled station, KSQ first.	Subclause 7.2.6	Always
Padding data	As required by the key wrap algorithm.	Subclause 8.2.3 and the algorithm specification.	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 15. The byte with index 0, having value 2b, shall be transmitted first.

Table 15 – 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 The output from the key wrap algorithm could be longer than the input. For instance, the AES Key Wrap Algorithm produces output that is exactly 8 octets longer than its input. Table 16 shows a typical example of the Wrapped Key Data using this algorithm.

Table 16 – Example of Wrapped Key Data

Data	Description	Size (in octets)
Session Key Length	So the controlled station will know what follows.	2
Control Direction Session Key	Using the minimum size 128-bit keys	16
Monitoring Direction Session Key		16
Key Status Message	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

WKD := OS8i[1..8i]; i:=WKL

7.2.8 Error message

7.2.8.1 Structure

Each Error message shall contain the information described in 7.2.8 and summarized in Table 17. An Error message shall indicate that the station did not accept the previous message from the other station. To avoid denial of service attacks, error messages shall be optional; any station may choose not to send them at any time.

It is recommended that Error messages also be transmitted on communications links other than the one on which the error occurred, in order to alert other controlling stations to possible attacks. It is also recommended that error messages be logged by both the sender and receiver.

Table 17 – Error message

Value	CSQ = Challenge Sequence number, or KSQ = Key Sequence number, defined in 7.2.2.2 or 7.2.6.2
Value	
Value	
Value	
Value	USR = User Number, defined in 7.2.8.3
Value	
Value	AID = Association ID, defined in 7.2.8.4
Value	
Enumerated value	ERR = Error code, defined in 7.2.8.5
As defined in the affected protocol	ETM = Error time stamp, defined in the affected protocol. This shall be an absolute and unambiguous timestamp of the time when the error was detected.
Value	ELN = Error length, defined in 7.2.8.6.
Value	
Number of octets specified in ELN	Error text, defined in 7.2.8.7

7.2.8.2 Sequence Number

This value shall be the CSQ or KSQ of the operation that the Error message is replying to.

7.2.8.3 User Number

This value shall be the USR of the operation that the Error message is replying to, identifying the set of Session Keys and the Update Key in use. The User Number may also be zero when the correct User Number is unknown, as described in 7.2.5.2.

7.2.8.4 Association ID

This value shall uniquely identify the association between controlled and controlling station on which the error occurred, in case the USR is not unique within the controlled station. The combination of USR and AID shall be unique within the controlled station. An Association ID of 0 shall indicate the statistic is being reported on the same association it is measuring.

AID := UI16[1..16]<0 ..65535>

7.2.8.5 Error code

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

ERR := UI8[1..8]<0..255>

<0> := not used

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

<2> := Unexpected reply. OBSOLETE, DO NOT USE. The other station transmitted a message that did not follow the procedures as described in 7.3.

<3> := No reply. OBSOLETE, DO NOT USE. The other station either did not respond to the Challenge message or did not follow an Aggressive Mode request with data for authentication.

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

<5> := MAC algorithm not permitted. The station sending this Error Code does not permit the use of the specified MAC algorithm on this link. Mandatory MAC algorithms are specified in 8.2.2.

<6> := Key Wrap algorithm not permitted. The station 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 8.2.3.

<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 controlled station does not permit the specified key change method on this link. Mandatory Update Key Change Methods are specified in 8.2.5.9.

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

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

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

<12...127>	:=	reserved for future standardization
<128..255>	:=	private range for definition by each vendor. A station 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.

7.2.8.6 Error Text Length

This value shall specify the length of the Error Text that follows.

ELN := UI16[1..16]<0 ..65535>

7.2.8.7 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 RFC 3629 (note that all characters encoded in 7-bit ASCII comply with UTF-8) . The Error Text shall explain the Error Code. For standardized Error Codes, the Error Text is optional and ELN may be zero. For private range Error Codes, the Error Text shall be mandatory. It is recommended that the error text contain a unique description of the user represented by the USR.

Error text := OS8i[1..8i]; i:=HLN

7.2.9 User Status Change message

7.2.9.1 Structure

Each User Status Change message shall either contain the information described in 7.2.9 and summarized in Table 18 and Table 19, or if an asymmetric key change method is used, may consist of an IEC/TS 62351-8 certificate, as described in 7.2.9.13.

A User Status Change message shall be transmitted by the controlling station to identify when a user of the controlled station has been added or deleted, when the user's role has changed, or when the date on which the user's access to the controlled station will expire has changed.

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

Prior to using this message, the choice to use either public keys or symmetric keys for remotely changing Update Keys shall be pre-configured at both controlling station and controlled station. This choice will determine the content of the Certification Data, as illustrated in Table 18.

Table 18 – 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 User Update Key Length (2 octets)	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 No key is transmitted in this case.

Table 19 – User Status Change message

Enumerated value	KCM = Key change method, defined in 7.2.9.2
Enumerated value	OPR = Operation, defined in 7.2.9.3
Value	SCS = Status Change Sequence Number, defined in 7.2.9.4
Value	
Value	
Value	
Value	URL = User role, defined in 7.2.9.5
Value	
Value	UEI = User role expiry interval, defined in 7.2.9.6
Value	
Value	UNL = User name length, defined in 7.2.9.7
Value	
Value	UKL = User public key length, defined in 7.2.9.8
Value	
Value	CDL = Certification data length, defined in 7.2.9.9
Value	
Number of octets specified in UNL	User name, defined in 7.2.9.10
Number of octets specified in UKL	User public key, defined in 7.2.9.11
Number of octets specified in CDL	Certification data, defined in 7.2.9.12

7.2.9.2 Key Change Method

The controlling station shall use this value to identify the method that will be used to change the Update Keys associated with the user. In this message, 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 algorithms identified here are described in more detail in 8.2. Values of Key Change Method 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.

KCM := UI8[1..8]<0..255>

<0> := reserved

<1> := reserved

<2> := reserved

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

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

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

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

<64> := reserved

<65> := reserved

<66> := reserved

<67> := Asymmetric RSA-2048 / 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 RS-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.

7.2.9.3 Operation

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

OPR := UI8[1..8]<0..255>

<0> := not used

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

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

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

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

7.2.9.4 Status Change Sequence Number

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.

SCS := UI32[1..32]<0.. 4294967295>

7.2.9.5 User Role

The controlling station 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 31 describes the permitted standard roles and the corresponding permissions. These roles are aligned with those defined in IEC/TS 62351-8. The interpretation of these permissions is a local issue. Controlled stations may be configured to disallow any of the standard roles defined here.

URL := UI16[1..16]<0 ..65535> see Table 31 for enumerations.

7.2.9.6 User Role Expiry Interval

The controlling station shall use this value to indicate when the role of this user will expire, causing the controlled station to invalidate the Update Key associated with this User Name. This value shall indicate the number of days after receiving the User Status Change message that the controlled station 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.

URL := UI16[1..16]<0 ..65535>

7.2.9.7 User Name Length

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

UNL := UI16[1..16]<0 ..65535>

7.2.9.8 User Public Key Length

The controlling station shall use this value to specify the length 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 and its length are NOT sent in the message.
- If the Key Change Method is between 64 and 127 inclusive, this value is the length of the User Public Key included in this message and signed by the authority.
- Any other values of Key Change Method are defined by external agreement and are not guaranteed to be interoperable.

UKL :=UI16[1..16]<0 ..65535>

7.2.9.9 Certification Data Length

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

CDL :=UI16[1..16]<0 ..65535>

7.2.9.10 User Name

The controlling station 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 "Default" shall be used to identify the default Update Key used between the controlling station and the controlled station. The format of the User Name is otherwise outside the scope of this specification.

User Name := OS8i[1..8i]; i:=UNL

7.2.9.11 User Public Key

The controlling station 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 message.

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

User Public Key := OS8i[1..8i]; i:=UKL

7.2.9.12 Certification Data

The authority shall use this value to certify that the other fields of this message are correct. The authority shall create the Certification Data as described in Table 18 using the specified Key Change Method and pass it to the controlling station for verbatim transmission to the controlled station in this field of this message.

Certification Data := OS8i[1..8i]; i:=CDL

7.2.9.13 User Status Change using a certificate

Instead of the User Status Change message described here, the controlling station and controlled station may optionally agree to use the X.509 certificates referred to as "access tokens" in IEC/TS 62351- 8 to change the status and role of the user. If they do so, they must provide an indication in the Protocol Implementation Conformance Statement that this option is being used. Support for use of the non-certificate User Status Change message shall be mandatory.

7.2.10 Update Key Change Request message

7.2.10.1 Structure

Each User Status Change message shall contain the information described in 7.2.10 and summarized in Table 20. The controlling station transmits this message to begin the process of changing the Update Key associated with a particular user at the controlled station. The controlling station specifies the name of the user whose Update Key is to be changed. The controlling station also includes pseudo-random challenge data to be used by the controlled station to authenticate itself.

The controlled station shall send an Update Key Change Reply message in response to this message.

Table 20 – Update Key Change Request message

Enumerated value	KCM = Key change method, defined in 7.2.9.2
Value	UNL = User name length, defined in 7.2.10.3
Value	
Value	CCL = Controlling station challenge data length, defined in 7.2.10.4
Value	
Number of octets specified in UNL	User name, defined in 7.2.10.5
Number of octets specified in CCL	CGC = Controlling station challenge data, defined in 7.2.10.6

7.2.10.2 Key Change Method

The controlling station 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 7.2.9.2. The controlling station shall use numbers smaller than 64 to specify symmetric algorithms and keys and numbers 64 to 127 specify asymmetric algorithms and keys.

7.2.10.3 User Name Length

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

UNL := UI16[1..16]<0 ..65535>

7.2.10.4 Controlling Station Challenge Data Length

The controlling station shall use this value to specify the length of the challenge data that follows. The minimum length shall be as specified in 8.2.5.9.

CCL := UI16[1..16]<4 ..65535>

7.2.10.5 User Name

The controlling station 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 "Default" shall be used to identify the common Update Key used between the controlling station and the controlled station. The format of the User Name is otherwise outside the scope of this specification.

User Name := OS8i[1..8i]; i:=UNL

7.2.10.6 Controlling Station Challenge Data

The controlling station shall send this data to avoid replay attacks on the changing of Update Keys. This value shall be pseudo-random data generated using the algorithm 3.1 specified in the *FIPS 186-2 Digital Signature Standard*.

CGC := OS8i[1..8i]; i:=CCL

7.2.11 Update Key Change Reply message

7.2.11.1 Structure

Each Update Key Change Reply message shall contain the information described in 7.2.11 and summarized in Table 21. This message is transmitted in response to an Update Key Change Request message. The controlled station uses this message to assign a sequence number to the Update Key change sequence, assign a User Number to the user in question, and supply the controlling station with pseudo-random challenge data.

Table 21 – Update Key Change Reply message

Value	KSQ = Key change sequence number, defined in 7.2.11.2
Value	
Value	
Value	
Value	USR = User number, defined in 7.2.11.3
Value	
Value	CDL = Challenge data length, defined in 7.2.11.4
Value	
Number of octets specified in CDL	CDC = Controlled station challenge data, defined in 7.2.11.5

7.2.11.2 Key Change Sequence Number (KSQ)

This is the Key Change Sequence number defined in the Session Key Status message (see 7.2.6). The controlled station 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 controlled station shall increment the KSQ each time it receives an Update Key Change Request message.

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

7.2.11.3 User Number

This value is the integer value the controlled station has chosen to represent the User Name specified in the Update Key Change Request message. The User Number need only be unique within the current communications link between the controlling station and the controlled station. Refer to 7.2.5.2 for the definition of User Numbers.

7.2.11.4 Controlled Station Challenge Data Length

This value defines the length of the challenge data that follows, in octets. The minimum value shall be as specified in 8.2.5.9.

CDL := UI16[1..16]<4 ..65535>

7.2.11.5 Controlled Station Challenge Data

The controlled station shall provide this pseudo-random data to ensure mutual authentication can take place between it and the controlling station. The pseudo-random data shall be generated using the algorithm 3.1 specified in the *FIPS 186-2 Digital Signature Standard*.

CDC := OS8i[1..8i]; i:=CDL

7.2.12 Update Key Change message

7.2.12.1 Structure

Each Update Key Change message shall contain the information described in 7.2.12 and summarized in Table 22. The controlling station uses this message to supply to the controlled station the encrypted new Update Key for a particular user.

This message shall be followed in the same ASDU by one of the following messages based on the Update Key Change Method specified by the controlling station in the Update Key Change Request.

- If the Update Key Change Method is symmetric, an Update Key Change Confirmation message follows.
- If the Update Key Change Method is asymmetric, an Update Key Change Signature message follows.

Table 22 – Update Key Change message

Value	KSQ = Key change sequence number, defined in 7.2.12.2
Value	
Value	
Value	
Value	USR = User number, defined in 7.2.12.3
Value	
Value	EUL = Encrypted update key length, defined in 7.2.12.4
Value	
Number of octets specified in EUL	EUD = Encrypted update key, defined in 7.2.12.5

7.2.12.2 Key Change Sequence Number

This is the Key Change Sequence number supplied by the controlled station in the Update Key Change Reply message (see 7.2.11.2).

7.2.12.3 User Number

This value is the integer value the controlled station has supplied in the Update Key Change Reply message (see 7.2.11.3) to represent the user whose Update Key is being changed.

7.2.12.4 Encrypted Update Key Length

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

EUL := UI16[1..16]<16..65535>

7.2.12.5 Encrypted Update Key Data

This value contains the new Update Key for the user, plus the name of the user and the Controlled station Challenge Data from the controlled station, in the order shown in Table 23.

Table 23 – Encrypted Update Key Data

Data	Description	From message…
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	
Controlled station Challenge Data	Pseudo-random data selected by the controlled station	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 controlled station. The controlling station shall pass this Encrypted Update Key Data from the central authority to the controlled station in this message without modification.
- If the Key Change Method is asymmetric, the Update Key Data shall be encrypted using the controlled station’s public key.
- **EUD** :=OS8i[1..8i]; i:=EUL

7.2.13 Update Key Change Signature message

7.2.13.1 Structure

Each Update Key Change Signature message shall contain the information described in 7.2.13 and summarized in Table 24. This message shall be transmitted by the controlling station only when the controlling station 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).

Table 24 – Update Key Change Signature message

Number of octets specified by the Key Change Method, defined in 7.2.9.2	Digital signature, defined in 7.2.13.2

7.2.13.2 Digital Signature

This value is the digital signature of the controlling station on behalf of the user, calculated over the data found in Table 25 in the order shown, using the algorithm specified in the Key Change Method of the Update Key Change Request.

The controlling station shall calculate the signature using the Private Key of the user, corresponding to the Public Key the controlling station supplied in the User Status Change message.

Table 25 – Data included in the Digital Signature

Data	Description	Source
Controlled station Name	The organizationally-unique name of the controlled station.	Pre-configured
Controlling Station Challenge Data	Pseudo-random data selected by the controlling station	Update Key Change Request
Controlled Station Challenge Data	Pseudo-random data selected by the controlled station	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 controlled station 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

Digital Signature :=OS8i[1..8i]; i:=defined by KCM

7.2.14 Update Key Change Confirmation message

7.2.14.1 Structure

Each Update Key Change Confirmation message shall contain the information described in 7.2.14 and summarized in Table 26. This message authenticates the controlling and controlled stations to each other using a message authentication code (MAC). Exchanging this message ensures that both controlling station and controlled station agree on the following information:

- the new Update Key,
- the name of the user or controlled station who is receiving the message,
- the pseudo-random challenge data provided by both controlling station and controlled station 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.

Table 26 – Update Key Change Confirmation message

Number of octets specified in Table 27	Message Authentication Code, defined in 7.2.14.2

7.2.14.2 Message Authentication Code

Table 27 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 controlling station in the Update Key Change message. 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 27 – Data included in the MAC calculation

Data	Description	From message…
Receiver’s User Name	Long organizationally-unique name for the user or controlled station whose is receiving this message.	If a controlling station is receiving this message, this name comes from the Update Key Change Request
		If a controlled station is receiving this message, the controlled station name was pre-configured.
Sender’s Challenge Data	If a controlling station is sending this message, this is the Controlling station Challenge Data	Update Key Change Request
	If an controlled station is sending this message, this is the Controlled station Challenge Data	Update Key Change Reply
Receiver’s Challenge Data	If a controlling station is receiving this message, this is the Controlling station Challenge Data	Update Key Change Request
	If an controlled station is receiving this message, this is the Controlled station 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 (USR)	Short number assigned by the controlled station to represent this user	Update Key Change Reply
Padding Data	Any padding data required.	n/a

MAC :=OS8i[1..8i]; i:=defined by Table 27

7.3 Formal procedures

7.3.1 Overview of subclause

Subclause 7.3 formally describes the procedures used by stations implementing this authentication mechanism as a part of each protocol. If 7.3 differs from Clause 6, 7.3 shall be considered definitive.

Table 28 describes the states used by the state machines in these procedures, in the general order in which they might be expected to occur. Refer to Figure 10 and Figure 11 for an overview of how the state machines work together.

Table 28 – States used in the state machine descriptions

State	Implemented in		Description	Refer to Table
	Controlling station	Controlled station		
Wait for Key Status	YES	No	The controlling station has either just initialized, or its Session Keys have expired. It has just transmitted a Request Key Status message and is waiting for the controlled station to transmit a Key Status message.	Table 32
Wait for Key Change Confirmation	YES	No	The controlling station has transmitted a Key Change message and is waiting for the controlled station to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK.	Table 32

State	Implemented in		Description	Refer to Table
	Controlling station	Controlled station		
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.	Table 30
Security Idle	YES	YES	There is no authentication in progress. The device is executing the standard protocol. The Session Keys may or may not be initialized.	Table 30
Wait for User Change Response	YES	No	The controlling station has transmitted a User Status Change message and is waiting for the controlled station to validate the Certification Data supplied by the authority indicating a change of status, role or Update Key for a user.	
Wait for Update Key Reply	YES	No	The controlling station has transmitted an Update Key Change Request and is waiting for an Update Key Change Reply from the controlled station.	
Wait for Update Key Confirm	YES	No	The controlling station has transmitted a Update Key Change and is waiting for an Update Key Change Confirmation from the controlled station.	

In each of these states except Security Idle, the station is waiting for a reply concerning a particular user. Stations 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.

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.

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

7.3.2 Security statistics

Stations shall monitor the use of the secure authentication mechanism by counting a variety of protocol events. Controlled stations shall report the totals using methods appropriate to the affected protocol. The methods used to store and report protocols shall permit counts of up to 4294967295 (32 bits).

Table 29 lists the security statistics and describes the event counted by each statistic.

Each controlled station shall maintain a local relative threshold for each statistic determining how often to report the statistic, as described in 8.2.5.3. 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 29 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.

A controlled station may report security statistics on communication links other than the one the statistics are measuring. This practice permits a controlling station to detect a potential attack on a different link by monitoring that link's statistics.

Each statistic, when reported by the controlled station, shall be accompanied by the Association ID representing the user/controlled station pair, as described in 7.2.8.4.

Table 29 –Security statistics

Name	Increment whenever...	Default threshold	Additional action
Unexpected Messages	The other station has responded with a message that was not the expected next step in the state machine.	3	Log each occurrence.
Authorization Failures	The other station 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.
Authentication Failures	The other station 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.
Reply Timeouts	The other station has not replied within the configured time required as described in 8.2.5.2.	3	If Max Reply Timeouts has been exceeded, cancel the current transaction.
Rekeys Due to Authentication Failure	An Authentication Failure has occurred that causes the controlling 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.
Total Messages Sent	The station sends an ASDU.	100	None.
Total Messages Received	The station receives an ASDU.	100	None.
Critical Messages Sent	The station sends an ASDU for what it assumes is a critical function. See 7.3.3.2 for a list of critical functions.	100	None.
Critical Messages Received	The station receives an ASDU for a critical function. See 7.3.3.2 for a list of critical functions.	100	None.
Discarded Messages	The station discards a received message.	10	None.
Error Messages Sent	The station has sent an Error message indicating an authentication failure or potential configuration error.	10	If Max Error Messages Sent has been exceeded, stop sending Error messages. Start sending Error messages again only if session keys are successfully changed.
Error Messages Rxed	The station has received an Error message.	10	None.
Successful Authentications	The station successfully authenticates a message.	100	None.

Name	Increment whenever...	Default threshold	Additional action
Session Key Changes	A user successfully changes session keys.	10	None.
Failed Session Key Changes	A user fails to change session keys	5	None.
Update Key Changes	The controlling station and authority change the Update Key for a user.	1	None.
Failed Update Key Changes	The controlling station and authority fail to change the Update Key for a user.	1	None.
Rekeys Due to Restarts	Only used by a controlling station. The controlling station reset the Session Keys because the controlled station restarted.	3	If Max Rekeys Due to Restarts has been exceeded, stop changing session keys due to controlled station restarts until the next Key Change Timeout.

7.3.3 Challenger procedures

7.3.3.1 Challenger role

A station, either controlling or controlled, that requires authentication from the other station 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 30.

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 30, the Challenger must have established a set of Session Keys using the Controlling Station state machine described in Table 32.

7.3.3.2 Critical functions

Each Challenger shall distinguish between Critical ASDUs and Non-Critical ASDUs. A Critical ASDU shall be a message implementing a critical function. A critical function is any function that the Challenger requires to be authenticated.

Controlled stations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical.

Changing any security parameters such as algorithms, key sizes, timeouts or intervals through the affected protocols shall be considered critical functions.

An additional minimum subset of critical functions for each affected protocol shall be defined in each protocol specification as specified in 10.3.

Challengers may optionally consider additional functions beyond this minimum subset to be critical.

7.3.3.3 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.

1) Stations shall set their CSQ to zero on startup.

2) Stations shall increment the CSQ each time they transmit a Challenge message.

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

4) Stations 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 station has transmitted since receiving the Challenge message. (Note rule 3 is a special case of rule 4).

5) A station 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:

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

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

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

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

8) If the affected protocol permits the controlled station to spontaneously transmit data, each station shall maintain two sets of Challenge data, one for Challenges sent in normal responses and one for Challenges sent spontaneously.

Examples of the effect of these rules are illustrated in Figure 14 Parts 1 and 2. The notation “Data=A”, “Data=B”, etc. indicates when the controlled station changes the Challenge Data and which instance of this data the controlling station uses to construct its Reply or Aggressive Mode Request.

Figure 14 Part 1 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 14 Part 2 illustrates a more complex case. Following the sequence in Figure 14 Part 1, the controlled station sends a spontaneous message at the same time the controlling station requests a critical operation. The messages cross in transit and the stations must use the CSQs to match transactions.

Following the example in Figure 14, one of the following cases may occur depending on what happens first:

- If the controlling station sends an Aggressive Mode Request, it will do so with CSQ=6 and Data=C, the last Challenge Data it received.
- If the controlling station sends a critical ASDU and the controlled station challenges it, the new Challenge will contain CSQ=6 and new Data=D.
- If the controlled station sends an unsolicited response containing a Challenge, the new Challenge will also contain CSQ=6 and new Data=D.

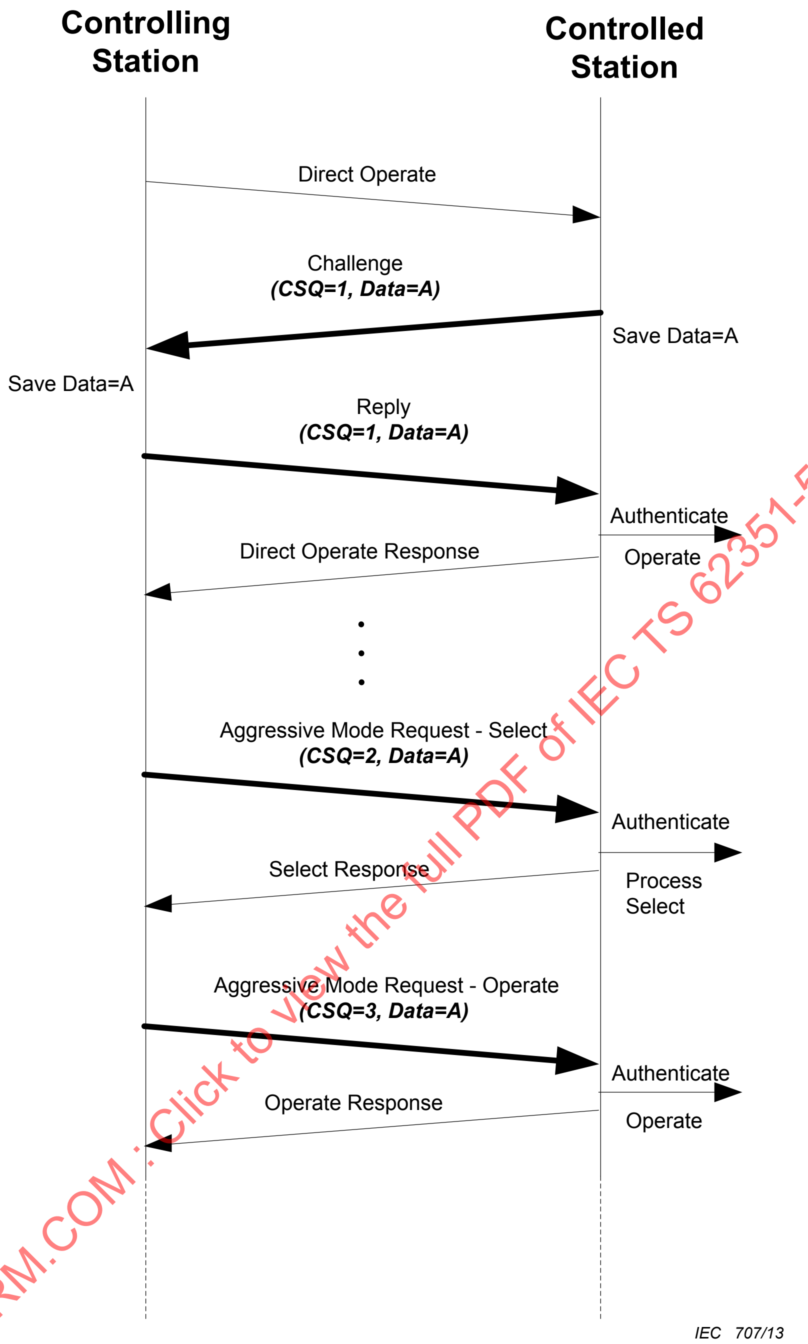

Figure 14 – Example Use of Challenge Sequence Numbers *(1 of 2)*

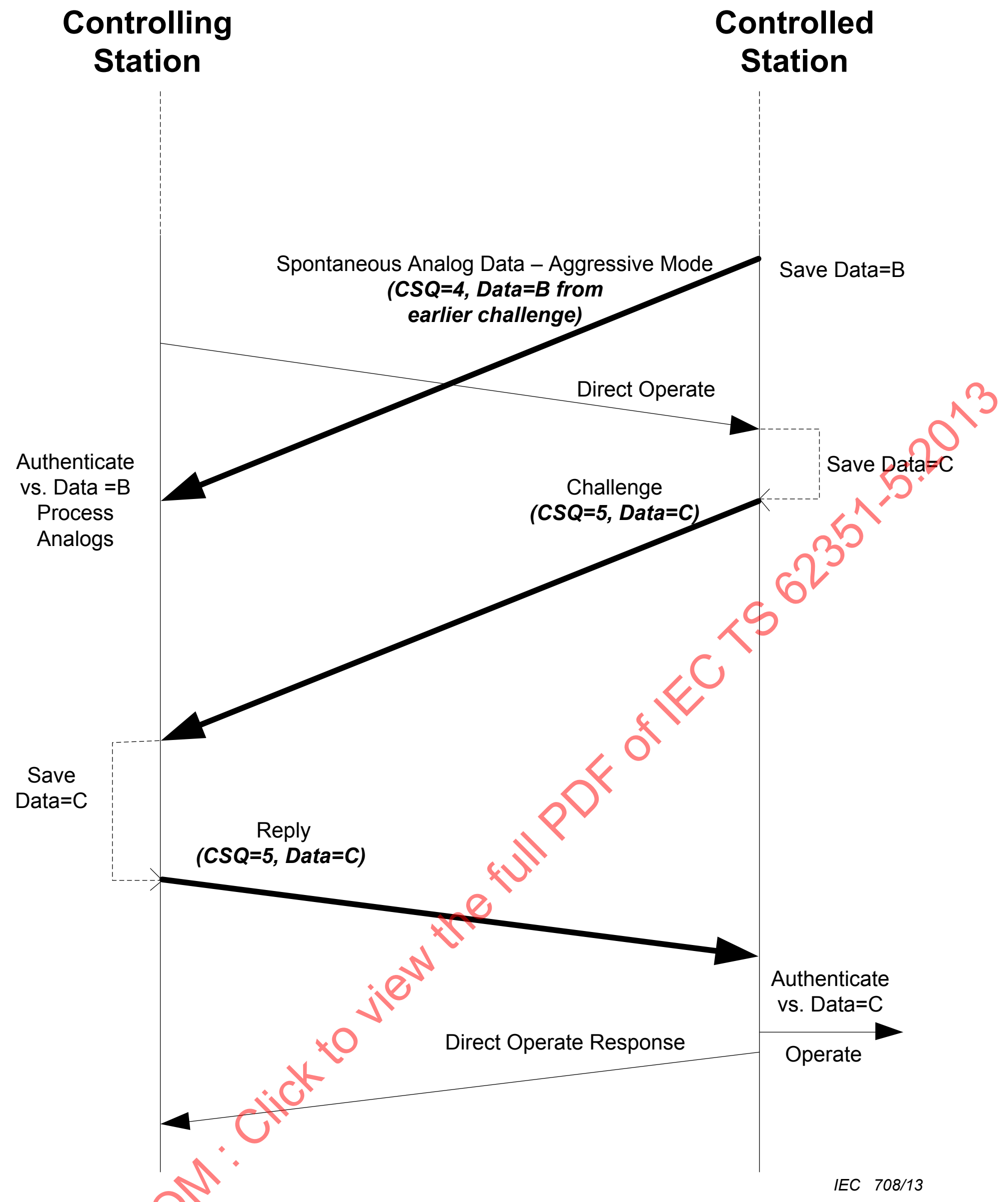

Figure 14 – Example Use of Challenge Sequence Numbers *(2 of 2)*

7.3.3.4 Authentication procedures

If the Challenger is in any of 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 7.2.3.5.

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 7.2.4.5. 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 7.2.4.3, 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.

7.3.3.5 Challenger state machine

Challengers (either controlling station or controlled station) shall implement the state machine described in Table 30. Note that whenever the controlled station 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.

NOTE Events or actions that only apply to one type of station or the other are identified by capitals as applying to “CONTROLLING STATION” or “CONTROLLED STATION”.

Table 30 – Challenger state machine

Event	Event description	State				
		Security Idle		**Wait for Reply**		
		The device is executing the standard protocol.		**The device is waiting for the other station to authenticate itself.**		
		Action	**Next state**	**Action**	**Next state**	
A	**B**	**C**	**D**	**E**	**F**	
Rx Unsolicited Non-Critical ASDU	CONTROLLING STATION only. The controlling station receives an unsolicited (spontaneous) 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx Critical ASDU	The Challenger receives an ASDU that requires authentication.	If (CONTROLLING STATION and Session Keys are valid) OR If CONTROLLED STATION: 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
		If CONTROLLING STATION 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 32)		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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
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
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 8.2.5.2 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 8.2.5.2 for details regarding the Reply Timer.	CONTROLLING STATION: Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 32)	CONTROLLING STATION: 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 32)	8

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
		CONTROLLED STATION: Set the current Key Status to COMM_FAIL. Reset Max Reply Timeouts.	Security Idle	CONTROLLED STATION: 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
Max Authentication Failures Exceeded	The Authentication Failures statistic has exceeded Max Authentication Failures. This may be due to an Rx Invalid Reply event, or a Rx Invalid Aggressive Mode Request event.	CONTROLLING STATION: 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 32)	CONTROLLING STATION: 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 32)	10
		CONTROLLING STATION or CONTROLLED STATION 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	CONTROLLING STATION or CONTROLLED STATION: 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
		CONTROLLED STATION: 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	CONTROLLED STATION: 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
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 CONTROLLING STATION only. Either the Key Change timer has expired, or The Key Change Count has been exceeded. Refer to 8.2.5.	Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Rekeys Due to Restarts	Wait for Key Status (Table 32)	Queue the event and process it after returning to Security Idle state.	Wait for Reply	14

7.3.3.5 Challenger state machine

Challengers (either controlling station or controlled station) shall implement the state machine described in Table 30. Note that whenever the controlled station 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.

NOTE Events or actions that only apply to one type of station or the other are identified by capitals as applying to “CONTROLLING STATION” or “CONTROLLED STATION”.

Table 30 – Challenger state machine

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx Unsolicited Non-Critical ASDU	CONTROLLING STATION only. The controlling station receives an unsolicited (spontaneous) 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx Critical ASDU	The Challenger receives an ASDU that requires authentication.	If (CONTROLLING STATION and Session Keys are valid) OR If CONTROLLED STATION: 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
		If CONTROLLING STATION 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 32)		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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
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
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 8.2.5.2 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 8.2.5.2 for details regarding the Reply Timer.	CONTROLLING STATION: Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Reply Timeouts.	Wait for Key Status (Table 32)	CONTROLLING STATION: 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 32)	8

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
		CONTROLLED STATION: Set the current Key Status to COMM_FAIL. Reset Max Reply Timeouts.	Security Idle	CONTROLLED STATION: 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
Max Authentication Failures Exceeded	The Authentication Failures statistic has exceeded Max Authentication Failures. This may be due to an Rx Invalid Reply event, or a Rx Invalid Aggressive Mode Request event.	CONTROLLING STATION: 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 32)	CONTROLLING STATION: 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 32)	10
		CONTROLLING STATION or CONTROLLED STATION 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	CONTROLLING STATION or CONTROLLED STATION: 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
		CONTROLLED STATION: 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	CONTROLLED STATION: 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
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 CONTROLLING STATION only. Either the Key Change timer has expired, or The Key Change Count has been exceeded. Refer to 8.2.5.	Transmit a Key Status Request Message. Start the Reply Timer. Reset Max Rekeys Due to Restarts	Wait for Key Status (Table 32)	Queue the event and process it after returning to Security Idle state.	Wait for Reply	14

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Expected Key Change Timeout	For CONTROLLED STATION only. The controlled station has not received a valid Key Change message within the Session Key Change interval or Session Key Change count configured at the controlled station. Refer to 8.2.5.	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
Rx Key Status Request	For CONTROLLED STATION only. The controlled station 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Expected Key Change Timeout	For CONTROLLED STATION only. The controlled station has not received a valid Key Change message within the Session Key Change interval or Session Key Change count configured at the controlled station. Refer to 8.2.5.	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
Rx Key Status Request	For CONTROLLED STATION only. The controlled station 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
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 CONTROLLED STATION 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
				IF Aggressive Mode is enabled for CONTROLLED STATION 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
				IF Aggressive Mode is enabled for CONTROLLING STATION 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. IF the Error Messages Sent statistic is <= Max Error Messages Sent,, transmit an Error Message with reason <4> Aggressive Mode Not Supported.	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
				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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
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
		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 <4> 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

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx Valid Key Change	For CONTROLLED STATION only. The controlled station 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 CONTROLLED STATION only. The controlled station 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 7.3.4.2	Security Idle	Reply as described in 7.3.4.2	Wait for Reply	26
Authority Changes User Status	For CONTROLLING STATION only. The controlling station receives from the authority some new Certification Data for a particular user.	IF the controlling station and controlled station support remotely changing Update Keys: Transmit the Certification Data in a new User Status Change message. Or user Certificate as appropriate. Start the Reply Timer.	Wait for User Change Response (Table 33)	Queue the event and process it after returning to Security Idle state.	Wait for Reply	27

Event	Event description	State				
		Security Idle		Wait for Reply		
		The device is executing the standard protocol.		The device is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Controlled Station Restarted	For CONTROLLING STATION only. The controlling receives an indication that the controlled station has restarted. 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 this event occurs, execute this row rather than the row that would be normally executed.	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 32)	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 32)	28
		IF Rekeys Due to Restarts > Max Rekeys Due to Restarts Discard ASDU containing the restart indication Increment Discarded Messages statistic	Security Idle	IF Rekeys Due to Restarts > Max Rekeys Due to Restarts Discard ASDU containing the restart indication Increment Discarded Messages statistic	Wait for Reply	29

7.3.3.6 Error messages

As described more formally in Table 30, stations may initially respond to error conditions by transmitting Error messages. To help protect against denial-of-service attacks, all stations shall stop transmitting Error messages after they have counted a number of errors that exceeds Max Error Messages Sent described in 8.2.5.3. Any station may also choose not to send Error messages at any time regardless of error count.

Error messages may be transmitted on communication links other than the one on which the error occurred. This practice can be extremely useful for detecting attacks and is therefore recommended. It is also recommended that all errors be logged.

7.3.4 Responder procedures

7.3.4.1 Responder role

A station, either controlling or controlled, that supplies authentication data shall be called a Responder. Each Responder shall follow the procedures described in 7.3.4.

7.3.4.2 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 8.2.5.2.

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.

7.3.4.3 Aggressive Mode

Aggressive Mode, in which a station supplies authentication information in the same ASDU as the data it is authenticating, shall be mandatory, but each station shall also provide a mode of operation in which Aggressive Mode can be configured as disabled.

A Responder that uses Aggressive Mode shall place a correctly-formed Aggressive Mode Request within the ASDU being authenticated. The location and the formatting of the Aggressive Mode Request within the ASDU shall be specific to the protocol and described in the specifications of the affected protocol.

A Responder shall not transmit an Aggressive Mode Request until it has successfully responded to at least one Challenge message each time the controlling station changes the Session Keys. In other words, the Responder shall send the first critical ASDU after a Session Key change as a normal protocol message, not as an Aggressive Mode Request.

7.3.4.4 Authentication errors

If the Responder receives an Error Message with reason <1> Authentication Failed after sending an Authentication Reply or Aggressive Mode Request message, 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 controlling station’s Session Key change interval or the controlled station’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.

1) A station shall not automatically retry sending an Aggressive Mode Request message if the controlling station sends an Error message.
2) If a user queues critical data for transmission by the controlling station and the controlling station is in Security Idle state, the controlling station shall transmit the data even if the last Key Status it received from the controlled station was not OK, i.e. the Session Keys are invalid and the controlling station was waiting for the Session Key change interval before changing the keys. If the controlled station then returns an Error message with reason <1> Authentication Failed, the controlling station 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.
3) If the controlling station 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.

7.3.5 Controlling station procedures

7.3.5.1 Controlling station role

In addition to acting as a Challenger and a Responder, controlling stations shall follow the procedures described in 7.3.5 in order to initialize and change user keys, status and roles at the controlled station.

7.3.5.2 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 2.

The controlled and controlling stations shall maintain a unique set of Session Keys for each user of the controlled station and a default set of Session Keys used for cases when the controlling station acts for multiple users (as in the case of a poll, for instance), or when the controlled station initiates the security message sequence.

Each controlling station shall initialize the Session Keys upon establishing communications or when it detects the controlled station has restarted, and periodically change the Session Keys as described in Table 32. The change interval shall be set using a configurable parameter as discussed in 8.2.5.3.

The controlling station shall use a symmetric Update Key to encrypt the Session Keys and transmit it to the controlled station in a Key Change message. An Update Key shall be separately assigned for each combination of user and controlled station. Each controlling station shall also act as a default user of the controlled station under the conditions described in Table 10. There shall be a separately assigned Update Key and set of Session Keys for that default user on the controlled station. It is possible for this default user to be the only user.

The controlling station shall consider an attack to be underway if the MAC on a Session Key Status message is found to be invalid using the most recent Monitoring Direction Session Key.

7.3.5.3 Deriving keys

All keys used in implementing this specification 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 the protocol is used. The key derivation algorithm chosen shall be an open standard, appropriate for the use being made of the protocol, consistent with the security policies of the organization implementing this specification and compliant with any regulatory requirements. Some recommended standards for key derivation are NIST SP 800-108 and ISO/IEC 18033-2:2006.

7.3.5.4 Assigning User Numbers

The controlling station and controlled station shall identify with a unique User Number each set of Session Keys that they share. The controlling station shall be responsible for initiating the assignment of User Numbers; the controlled station 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 controlled station.

Note that the controlled station 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 controlled and controlling stations also use a second reserved User Number <1> as the default User Number in a number of different situations, as described in 7.2.5.2.

7.3.5.5 Changing User Status

A controlling station or controlled station may optionally permit remotely changing Update Keys using the affected protocol. 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 controlling station or controlled station 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 11770-2 and ISO/IEC 11770-3 standards. Annex A 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 7.3.5.5.

If the controlling station and controlled station both permit remotely changing Update Keys, the controlling station shall promptly inform the controlled station of changes made by an authority to the status of a user and to the user’s Update Keys, as described in Table 33.

The authority shall *not* be the controlling station itself, but is otherwise not described by this specification. The communication between the authority and the controlling station shall be secured but is assumed to be a protocol suite other than the affected protocol. It is therefore not discussed in this specification. 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 specification.

The authority may add users, delete users or change the information associated with a user via the controlling station. The information associated with each user (known as the Certification Data) shall be specified in the User Status Change message or certificate, 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 “Default” shall be used to identify the default Update Key, User Number <1>, used between the controlling station and the controlled station. The format of the User Name is otherwise outside the scope of this specification.
- 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 controlled station, as described in Table 31. These roles are defined inn IEC/TS 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 controlling station shall provide the new Update Key to the controlled station in a confidential, authenticated manner as described in Table 33. If the Update Key Change Method is asymmetric, the controlling station first shall supply the user’s Public Key to the controlled station, unencrypted but digitally signed by the authority using the Authority Private Key, in the User Status Change message. This User Public Key will later be used to decrypt the Update Key.
- Expiry Interval. The authority may change the time when the Role of the user and the validity of the Update Key will expire.

Table 31 – 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	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.						

The authority, controlling station, and controlled station 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 messages, shall be preconfigured at the controlling station as described in 8.2.5.9, and the controlling station shall specify it to the controlled station in the User Status Change message.

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

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 controlling station with Certification Data for the default user before the controlling station begins communicating with the controlled station. If the controlled station is not pre-configured with the default user, the controlling station shall add that user before beginning secure communications with the controlled station.

7.3.5.6 Changing Update Keys

If the controlling station and controlled station both permit remotely changing Update Keys, the controlling station 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 message or certificate. The controlling station shall do so by sending an Update Key Change Request message containing the User Name of the user and some random challenge data. It is recommended that the controlling station 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 controlling station completes this process.

Upon receiving an Update Key Change Reply message from the controlled station, the controlling station shall obtain the Encrypted Update Key Data to send to the controlled station in an Update Key Change message. As described in the definition of that message, the Encrypted Update Key Data shall consist of the following data, encrypted together:

- the name of the user;
- the random challenge data sent from controlled station in the Update Key Change Reply;
- the new Update Key for the user.

The controlling station 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 controlling station shall obtain the Encrypted Update Key Data from the authority. The method used to do so is outside the scope of this specification but the communication must be secured. The authority shall encrypt the Update Key Data using the symmetric key it shares with the controlled station (i.e. the Authority Certification Key described in Table 2). The controlling station shall authenticate the transfer of the Encrypted Update Key Data by sending an Update Key Change Confirmation message with the Update Key Change message in its request. In this way, the controlling station authenticates the transfer of the Encrypted Update Key Data using the new Update Key itself. The authority securely provided the controlled station with the Update Key in the User Status Change message, so the controlled station can verify that the controlling station is authentic and the controlling station and authority agree on the new Update Key.
- If the Update Key Change Method is asymmetric, the controlling station shall create the Encrypted Update Key Data using the controlled station’s Public Key. The controlling station shall authenticate the transfer of the Encrypted Update Key Data by sending an Update Key Change Signature message with the Update Key Change message in its request. In this way, the controlling station authenticates the transfer of the Encrypted Update Key Data by signing it with the User’s Private Key. The authority securely provided the controlled station with the User’s Public Key in the User Status Change message, so the controlled station can verify that the controlling station is authentic and the controlling station and the authority agree on the new Update Key.

- Using either method, if the controlling station does not wish to actually change the Update Key, it can instead authenticate itself to the controlled station and verify that the controlled station has the correct Update Key by sending only an Update Key Change Confirmation message, which will cause the controlled station to reply with an Update Key Change Confirmation.

Upon receiving an Update Key Change Confirmation message from the controlled station, the controlling station shall verify that the Message Authentication Code (MAC) in that message is valid. The master calculates this MAC using the random challenge data from both itself and the controlled station, the user's name, the User Number (USR) and the Key Change Sequence Number (KSQ). If the MAC is valid, the controlling station 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 33, the controlling station 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 specification.

7.3.5.7 Controlling Station State Machine

The controlling station shall execute the state machines in Table 32 and Table 33.

Table 32 – Controlling Station State Machine – Changing Session Keys

Event	Event description	State				
		Wait for Key Status		**Wait for Key Change Confirmation**		
		The controlling station is waiting for the controlled station to send any Key Status message.		The controlling station is waiting for the controlled station 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 controlling station 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 controlling station 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 controlling station 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 controlling station was waiting for a response from the controlled station.	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**

Event	Event description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The controlling station is waiting for the controlled station to send any Key Status message.		The controlling station is waiting for the controlled station 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	
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 8.2.5.2 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
Key Change Timeout	Either the Key Change Timer has expired on the controlling station, 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 controlling station 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

<table>
<tr><th rowspan="4">Event</th><th rowspan="4">Event description</th><th colspan="4">State</th><th rowspan="5"></th></tr>
<tr><th colspan="2">Wait for Key Status</th><th colspan="2">Wait for Key Change Confirmation</th></tr>
<tr><td colspan="2">The controlling station is waiting for the controlled station to send any Key Status message.</td><td colspan="2">The controlling station is waiting for the controlled station to send confirmation that the Key Change has been accepted, by transmitting a Key Status message with the Key Status = <1> OK</td></tr>
<tr><th>Action</th><th>Next state</th><th>Action</th><th>Next state</th></tr>
<tr><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>F</th></tr>
<tr><td>Rx Critical ASDU</td><td>The controlling station receives an ASDU that requires authentication even though the Session Keys are not yet valid.</td><td>Increment Unexpected Messages statistic.
Increment Authentication Failures statistic.
Discard the Critical ASDU.
Increment Discarded Messages statistic.</td><td>Wait for Key Status</td><td>Increment Unexpected Messages statistic.
Increment Authentication Failures statistic.
Discard the Critical ASDU.
Increment Discarded Messages statistic.</td><td>Wait for Key Change Confirmation</td><td>8</td></tr>
<tr><td>Rx Unsolicited Non-Critical ASDU</td><td>The controlling station receives an ASDU that does not require authentication and was spontaneously transmitted by the controlled station.</td><td>Process the ASDU and issue a Confirm if required.</td><td>Wait for Key Status</td><td>Process the ASDU and acknowledge it if required</td><td>Wait for Key Change Confirmation</td><td>9</td></tr>
<tr><td>Rx Inappropriate Non-Critical ASDU</td><td>The controlling station receives a non-critical, non-authentication ASDU in response to its previous authentication message, or receives some other indication that the controlled station may not be capable of processing authentication messages.</td><td>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.</td><td>Security Idle</td><td>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.</td><td>Security Idle</td><td>10</td></tr>
<tr><td>A User Wants to Transmit an ASDU</td><td>A user wishes to transmit from this controlling station. May be either a critical or non-critical ASDU.</td><td>Queue the ASDU until the next time the controlling station enters Security Idle state.</td><td>Wait for Key Status</td><td>Queue the ASDU until the next time the controlling station enters Security Idle state.</td><td>Wait for Key Change Confirmation</td><td>11</td></tr>
</table>

Event	Event description	State				
		Wait for Key Status		Wait for Key Change Confirmation		
		The controlling station is waiting for the controlled station to send any Key Status message.		The controlling station is waiting for the controlled station 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 Unexpected Key Status	The controlling station 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 controlled station 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
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 Controlling station has just restarted, so the session keys are not yet valid and the Controlling station 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 controlling station 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 33 – Controlling Station State Machine – Changing Update Keys

Event	State						
	Wait for User Change Response		Wait for Update Key Reply		Wait for Update Key Confirmation		
	The controlling station is waiting for the controlled station to send a response to a User Status Change request.		The controlling station is waiting for the controlled station to reply to an Update Key Change request.		The controlling station is waiting for the controlled station to send an Update Key Confirmation response.		
	Action	Next State	Action	Next State	Action	Next State	
A	C	D	E	F	G	H	
Rx No-Error Response	IF the User Status Change must be applied immediately, Transmit Update Key Change Request. 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	Discard the Reply. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	Wait for User Change Response	Transmit Signed Update Key Change and either Update Key Change Signature or Update Key Change Confirmation. OR Transmit only an Update Key Change Confirmation. Restart the Reply Timer. Reset Max Reply Timeouts.	Wait for Update Key Confirmation	Transmit Signed Update Key Change and either Update Key Change Signature or Update Key Change Confirmation. OR Transmit only an Update Key Change Confirmation Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Confirmation	2

Event	State						
	Wait for User Change Response		Wait for Update Key Reply		Wait for Update Key Confirmation		
	The controlling station is waiting for the controlled station to send a response to a User Status Change request.		The controlling station is waiting for the controlled station to reply to an Update Key Change request.		The controlling station is waiting for the controlled station to send an Update Key Confirmation response.		
	Action	Next State	Action	Next State	Action	Next State	
A	C	D	E	F	G	H	
Rx Valid Update Key Change Confirmation	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	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 message 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 controlling station is waiting for the controlled station to send a response to a User Status Change request.		The controlling station is waiting for the controlled station to reply to an Update Key Change request.		The controlling station is waiting for the controlled station to send an Update Key Confirmation response.		
	Action	Next State	Action	Next State	Action	Next State	
A	C	D	E	F	G	H	
Reply Timeout	Transmit User Status Change. Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for User Change Response	Transmit Update Key Change Request. Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Reply	Transmit Update Key Change message and either Update Key Change Signature message or Update Key Change Confirmation message in same ASDU. OR Transmit only an Update Key Change Confirmation. Restart the Reply Timer. Increment Reply Timeouts Statistic.	Wait for Update Key Confirmation	5
MaxReply Timeouts Exceeded	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	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 Confirmation	7
Rx Error	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	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for User Change Response	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for Update Key Reply	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for Update Key Confirmation	9

Event	State						
	Wait for User Change Response		Wait for Update Key Reply		Wait for Update Key Confirmation		
	The controlling station is waiting for the controlled station to send a response to a User Status Change request.		The controlling station is waiting for the controlled station to reply to an Update Key Change request.		The controlling station is waiting for the controlled station to send an Update Key Confirmation response.		
	Action	Next State	Action	Next State	Action	Next State	
A	C	D	E	F	G	H	
A User Wants to Transmit an ASDU	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for User Change Response	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for Update Key Reply	Queue the ASDU until the next time the controlling station enters Security Idle state.	Wait for Update Key Confirmation	10
Rx Unsolicited Non-Critical ASDU	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	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 Confirmation	12

7.3.6 Controlled station procedures

7.3.6.1 Controlled station role

In addition to acting as a Challenger and a Responder, each controlled station shall follow the procedures described in 7.3.6, permitting the Controlling station to initialize and change Session Keys and to change the status, Role, Expiry Interval and Update Keys of users.

7.3.6.2 Key Status

The controlled station shall maintain an internal variable having the possible values of Key Status described in 7.2.6.5, and return this value in reply to each Key Status Request Message. The controlled station shall set the Key Status to <1> NOT_INIT upon startup of the controlled station.

If the number of Key Status Request messages received by the controlled station exceeds a configured threshold within the Expected Session Key Timeout, the controlled station shall notify a human as described in 8.2.5.7.

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

7.3.6.3 Authenticating Session Key Changes

Upon receiving a Key Change message, the controlled station 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 controlled station, the controlled station 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 controlled station, the controlled station shall consider the Key Change message invalid.

7.3.6.4 Changing Session Keys

A controlled station shall respond to a Key Change message within an acceptable Reply Timeout defined per system as described in 8.2.5.2.

A controlled station 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 a configured interval, as described in 8.2.5.6.

7.3.6.5 Changing User Status

Upon receiving a User Status Change message or a certificate, the controlled station shall validate the Certification Data (including User Name, Role, Expiry Interval and new Update Key or public key for the user) in that message as follows:

- Verify that the controlled station supports the specified Update Key Change Method (described in 8.2.5.9).
- Verify that the Certification Data was created by the authority, using the authority's credentials that were pre-configured at the controlled station:
  - If the Update Key Change Method is symmetric, validate the MAC of the Certification Data using the symmetric key shared between the controlled station and the authority.
  - If the Update Key Change Method is asymmetric, validate the authority's digital signature against the authority's public key.