

PD IEC/TS 62351-5:2013



BSI Standards Publication

Power systems management and associated information exchange — Data and communications security

Part 5: Security for IEC 60870-5
and derivatives

bsi.

...making excellence a habit.
AVA **Documents**
Document Sharing Hub

National foreword

This Published Document is the UK implementation of IEC/TS 62351-5:2013. It supersedes DD IEC/TS 62351-5:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014.
Published by BSI Standards Limited 2014

ISBN 978 0 580 78904 5
ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 August 2014.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



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

PRICE CODE **XE**

ICS 33.200

ISBN 978-2-83220-732-1

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

CONTENTS

FOREWORD.....	6
1 Scope and object.....	8
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	11
5 Problem description (informative)	11
5.1 Overview of clause	11
5.2 Specific threats addressed	11
5.3 Design issues.....	11
5.3.1 Overview of subclause.....	11
5.3.2 Asymmetric communications.....	11
5.3.3 Message-oriented	12
5.3.4 Poor sequence numbers or no sequence numbers.....	12
5.3.5 Limited processing power	12
5.3.6 Limited bandwidth.....	12
5.3.7 No access to authentication server	12
5.3.8 Limited frame length	13
5.3.9 Limited checksum	13
5.3.10 Radio systems	13
5.3.11 Dial-up systems.....	13
5.3.12 Variety of protocols affected	13
5.3.13 Differing data link layers	14
5.3.14 Long upgrade intervals	14
5.3.15 Remote sites	14
5.3.16 Multiple users	14
5.3.17 Unreliable media	14
5.4 General principles	14
5.4.1 Overview of subclause.....	14
5.4.2 Authentication only	14
5.4.3 Application layer only	15
5.4.4 Generic definition mapped onto different protocols	15
5.4.5 Bi-directional	15
5.4.6 Challenge-response.....	15
5.4.7 Pre-shared keys as default option.....	15
5.4.8 Backwards tolerance	15
5.4.9 Upgradeable.....	16
5.4.10 Perfect forward secrecy.....	16
5.4.11 Multiple users and auditing	16
6 Theory of operation (informative).....	16
6.1 Overview of clause	16
6.2 Narrative description	16
6.2.1 Basic concepts	16
6.2.2 Initiating the challenge.....	17
6.2.3 Replying to the challenge	17
6.2.4 Authenticating	18
6.2.5 Authentication failure.....	18

6.2.6	Aggressive mode	18
6.2.7	Changing keys	18
6.2.8	Security statistics	22
6.3	Example message sequences	22
6.3.1	Overview of subclause	22
6.3.2	Challenge of a Critical ASDU	23
6.3.3	Aggressive Mode	24
6.3.4	Initializing and changing Session Keys	24
6.4	State machine overview	28
7	Formal specification	32
7.1	Overview of clause	32
7.2	Message definitions	32
7.2.1	Distinction between messages and ASDUs	32
7.2.2	Challenge message	33
7.2.3	Reply message	35
7.2.4	Aggressive Mode Request message	36
7.2.5	MAC := OS8i[1..8i]; i:=specified by MALKey Status Request message	38
7.2.6	Key Status message	38
7.2.7	Session Key Change message	41
7.2.8	Error message	43
7.2.9	User Status Change message	45
7.2.10	Update Key Change Request message	49
7.2.11	Update Key Change Reply message	51
7.2.12	Update Key Change message	52
7.2.13	Update Key Change Signature message	53
7.2.14	Update Key Change Confirmation message	54
7.3	Formal procedures	55
7.3.1	Overview of subclause	55
7.3.2	Security statistics	56
7.3.3	Challenger procedures	58
7.3.4	Responder procedures	74
7.3.5	Controlling station procedures	75
7.3.6	Controlled station procedures	88
8	Interoperability requirements	90
8.1	Overview of clause	90
8.2	Minimum requirements	90
8.2.1	Overview of subclause	90
8.2.2	MAC algorithms	90
8.2.3	Key wrap / transport algorithms	91
8.2.4	Fixed values	91
8.2.5	Configurable values	91
8.3	Options	96
8.3.1	Overview of subclause	96
8.3.2	MAC algorithms	96
8.3.3	Encryption algorithms	98
8.3.4	Key wrap / transport algorithms	98
8.3.5	Configurable values	98
9	Special Applications	

9.1	Overview of clause	99
9.2	Use with TCP/IP	99
9.3	Use with redundant channels.....	99
9.4	Use with external link encryptors	99
10	Requirements for referencing this specification.....	99
10.1	Overview of clause	99
10.2	Selected options.....	99
10.3	Operations considered critical	100
10.4	Addressing information.....	100
10.5	Message format mapping	100
10.6	Reference to procedures	100
11	Protocol implementation conformance statement.....	101
11.1	Overview of clause	101
11.2	Required algorithms	101
11.3	MAC algorithms.....	101
11.4	Key wrap algorithms.....	101
11.5	Maximum Error messages sent.....	101
11.6	Use of Error messages	101
11.7	Update Key Change Methods	102
11.8	User Status Change	102
Annex A	(informative) Compliance with ISO/IEC 11770.....	103
Bibliography		109
Figure 1	– Overview of interaction between Authority and stations	22
Figure 2	– Example of successful Challenge of Critical ASDU	23
Figure 3	– Example of failed Challenge of Critical ASDU	23
Figure 4	– Example of a successful Aggressive Mode Request	24
Figure 5	– Example of a failed Aggressive Mode Request.....	24
Figure 6	– Example of Session Key initialization and periodic update.....	25
Figure 7	– Example of communications failure followed by Session Key change	26
Figure 8	– Example of successful User Status and Update Key Change	27
Figure 9	– User changes controlling stations.....	28
Figure 10	– Major state transitions for controlling station authentication.....	29
Figure 11	– Major state transitions for controlled station authentication	30
Figure 12	– Major state transitions for controlling station Update Key change	31
Figure 13	– Major state transitions for controlled station Update Key change	32
Figure 14	– Example Use of Challenge Sequence Numbers.....	60
Table 1	– Scope of application to standards.....	8
Table 2	– Summary of symmetric keys used	18
Table 3	– Summary of asymmetric keys used (optional).....	19
Table 4	– Challenge message.....	33
Table 5	– Reply message	35
Table 6	– Data Included in the MAC Value calculation	36
Table 7	– Aggressive Mode Request message.....	36

Table 8 – Data Included in the MAC Value calculation in Aggressive Mode.....	37
Table 9 – Key Status Request Message.....	38
Table 10 – Use of Default Session Keys	38
Table 11 – Key Status Message.....	39
Table 12 – Data Included in the MAC Value Calculation for Key Status.....	41
Table 13 – Key Change message.....	41
Table 14 – Data Included in the key wrap (in order)	42
Table 15 – Example of key order.....	42
Table 16 – Example of Wrapped Key Data.....	43
Table 17 – Error message.....	43
Table 18 – Creation of Certification Data	46
Table 19 – User Status Change message	46
Table 20 – Update Key Change Request message.....	50
Table 21 – Update Key Change Reply message.....	51
Table 22 – Update Key Change message	52
Table 23 – Encrypted Update Key Data	53
Table 24 – Update Key Change Signature message	53
Table 25 – Data included in the Digital Signature.....	54
Table 26 – Update Key Change Confirmation message.....	54
Table 27 – Data included in the MAC calculation	55
Table 28 – States used in the state machine descriptions	55
Table 29 –Security statistics	57
Table 30 – Challenger state machine	63
Table 31 – User roles	77
Table 32 – Controlling Station State Machine – Changing Session Keys.....	80
Table 33 – Controlling Station State Machine – Changing Update Keys	84
Table 34 – Special Statistic Event Thresholds.....	92
Table 35 – Algorithms and Messages used for each Update Key Change Method	94
Table 36 – Size of Challenge Data.....	94
Table 37 – Configuration of Cryptographic Information.....	95
Table 38 – Legend for configuration of cryptographic information.....	96
Table 39 – Construction of AES-GMAC initialization vector	96
Table 40 – Source of initialization vector components in each message.....	97
Table A.1 – Cryptographic Notation	105
Table A.2 – Compliance with ISO/IEC 11770	107

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 mess-

ages 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.

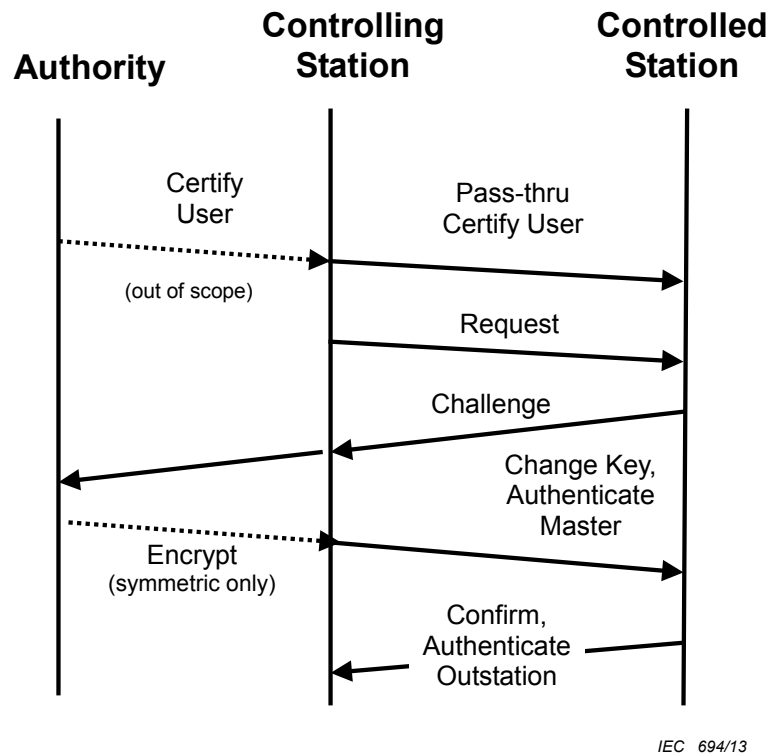


Figure 1 – Overview of interaction between Authority and stations

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.

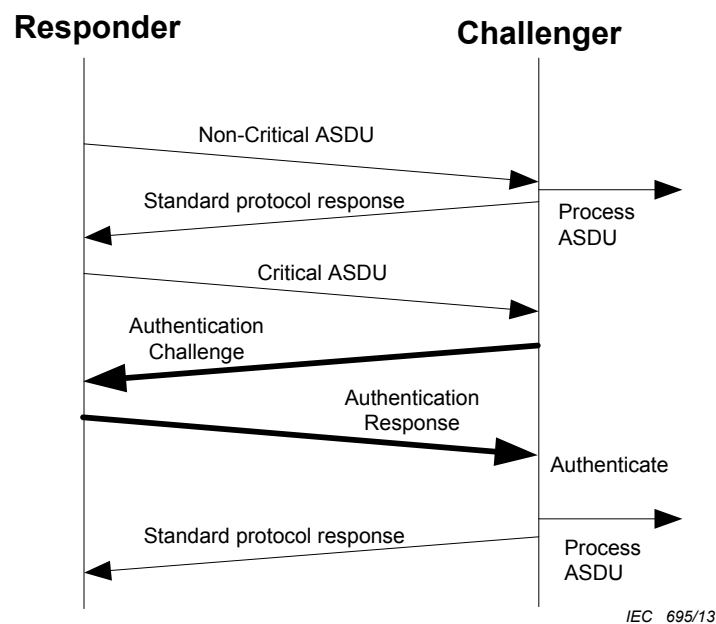


Figure 2 – Example of successful Challenge of Critical ASDU

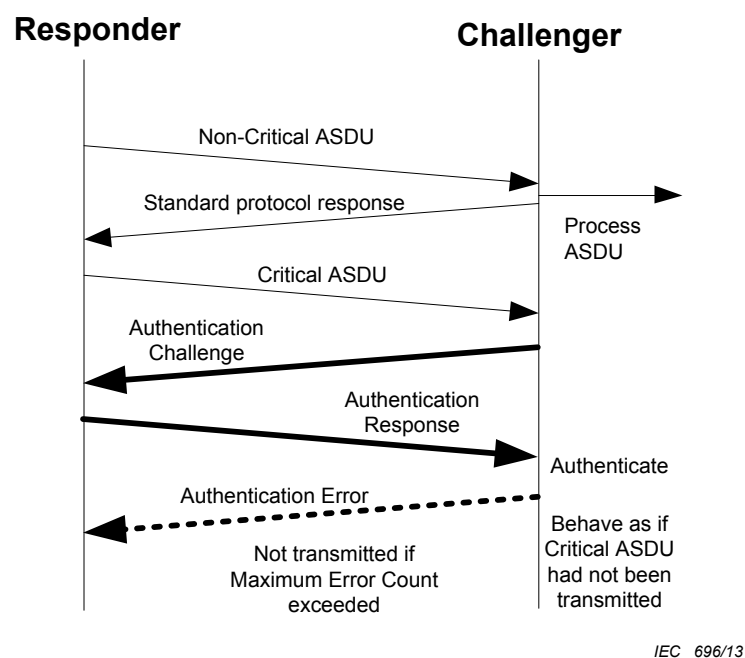


Figure 3 – Example of failed Challenge of Critical ASDU

6.3.3 Aggressive Mode

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

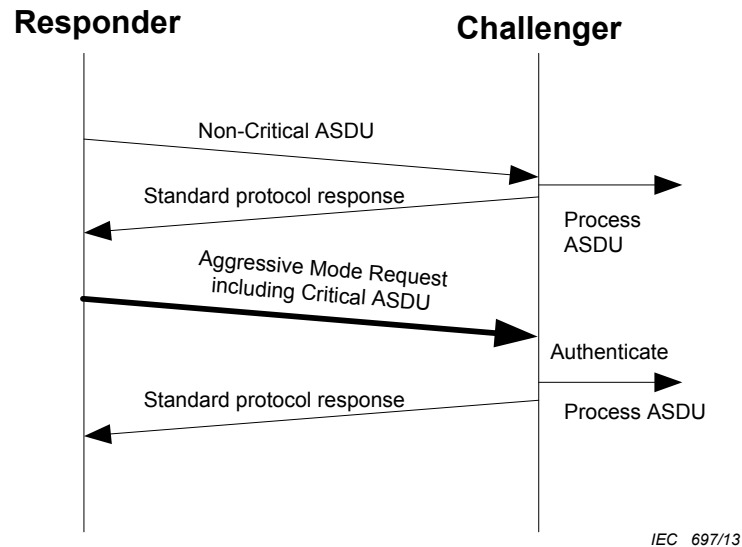


Figure 4 – Example of a successful Aggressive Mode Request

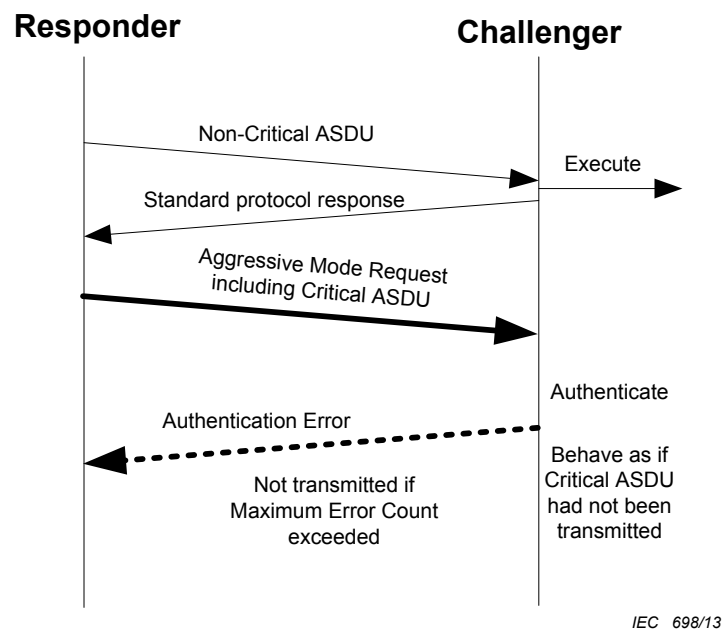


Figure 5 – Example of a failed Aggressive Mode Request

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.

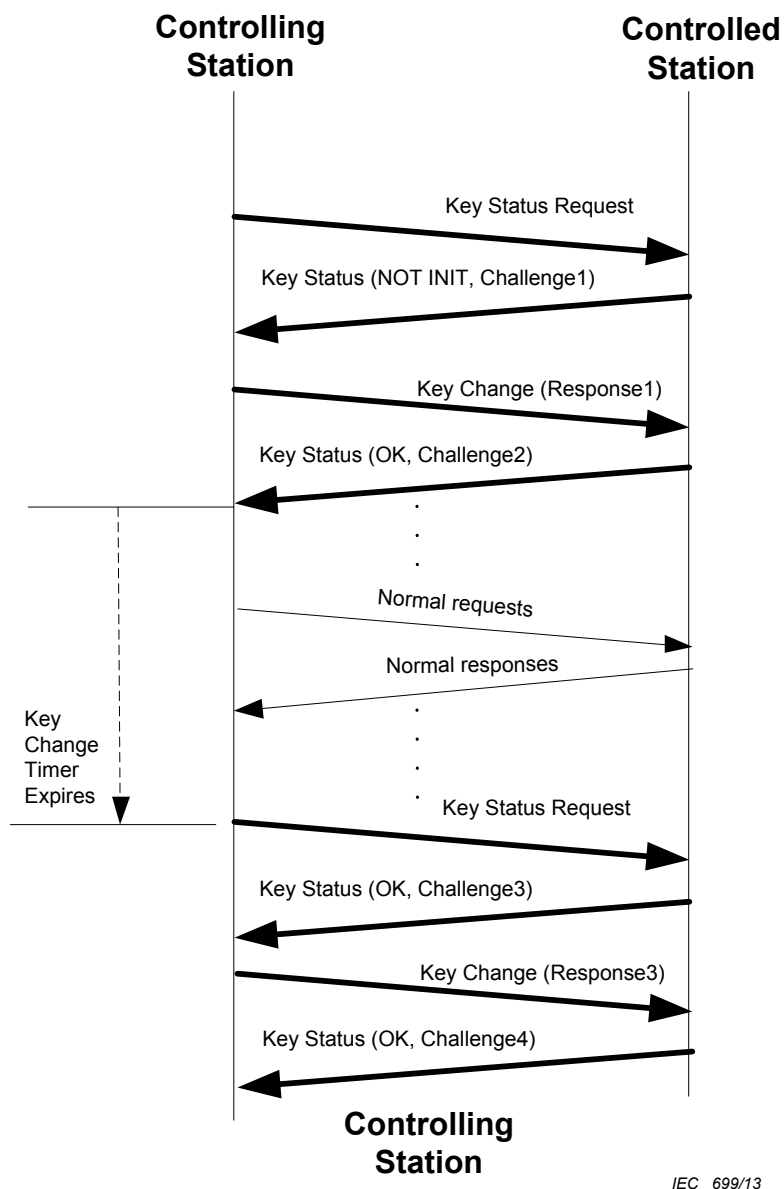
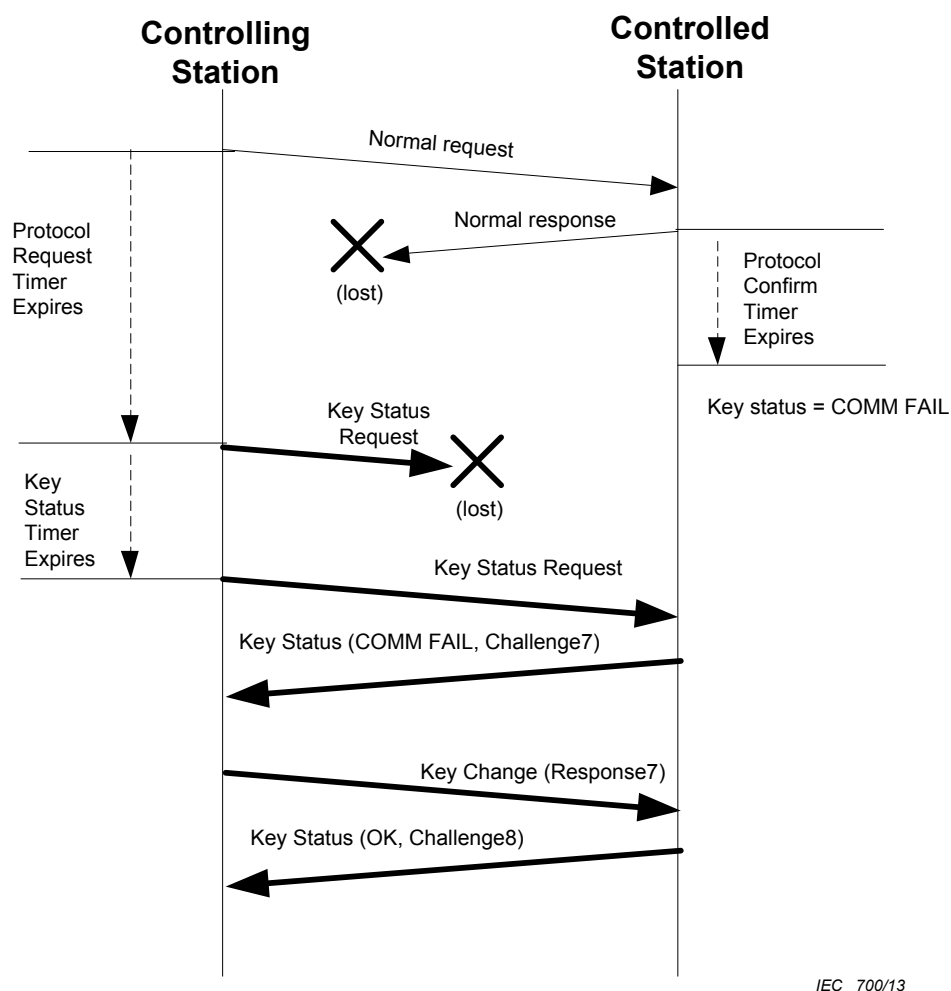
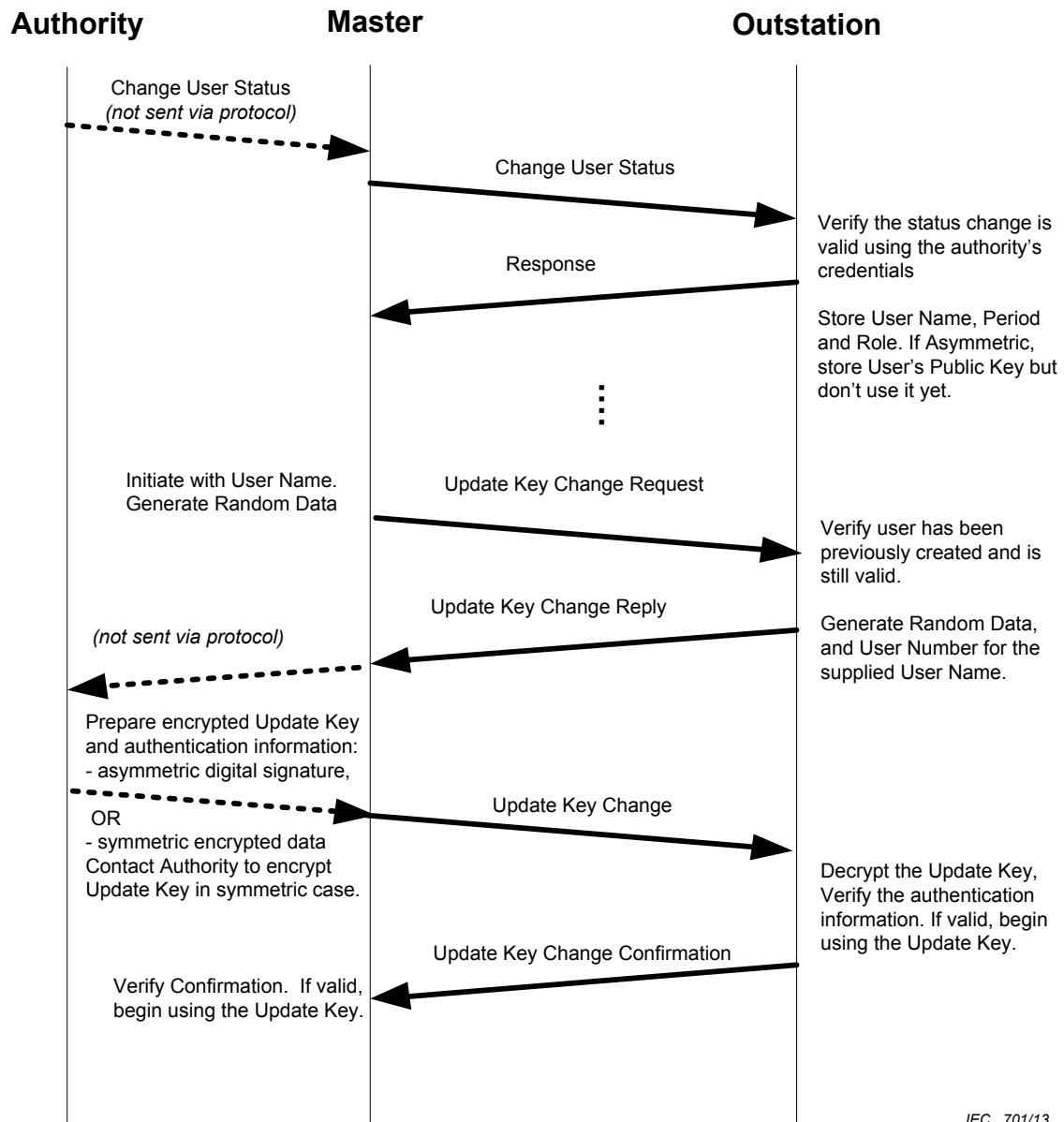


Figure 6 – Example of Session Key initialization and periodic update



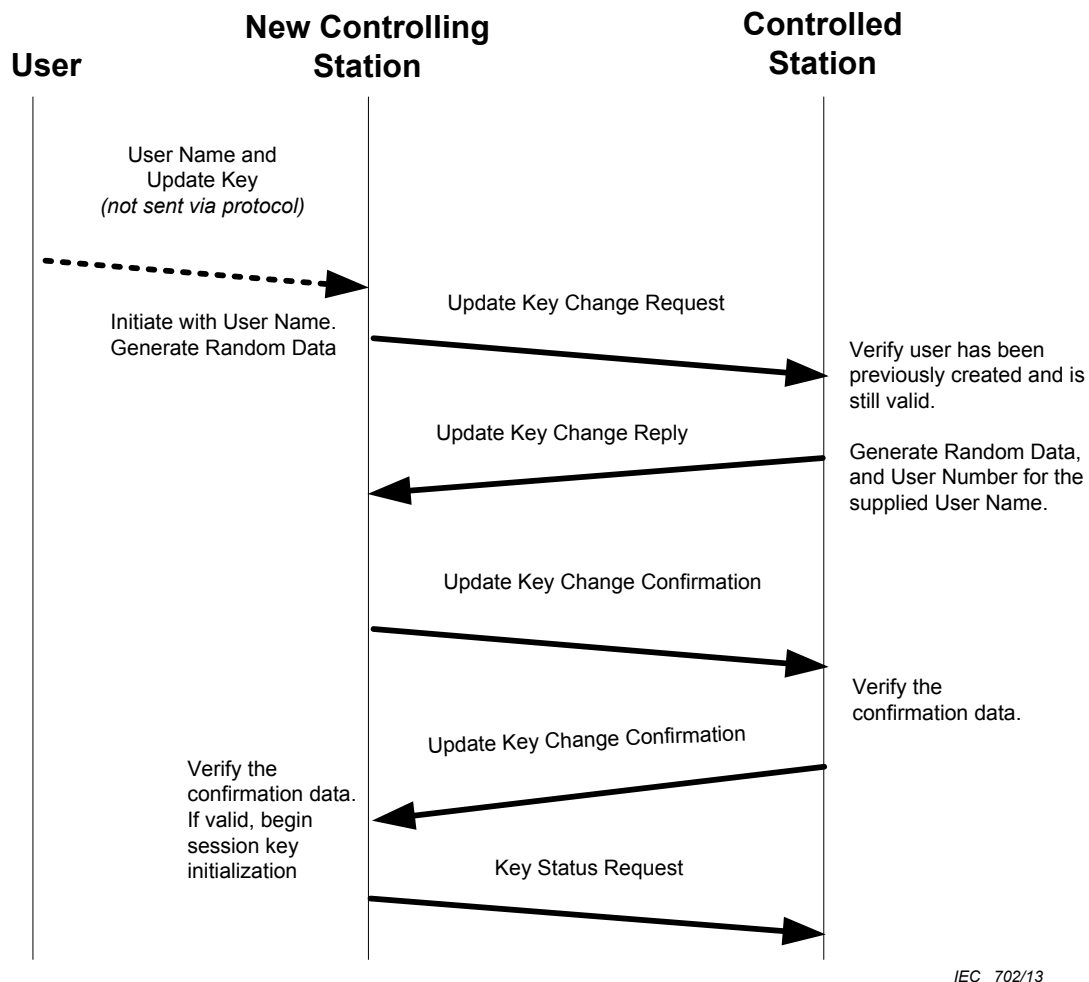
IEC 700/13

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



IEC 701/13

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



IEC 702/13

Figure 9 – User changes controlling stations

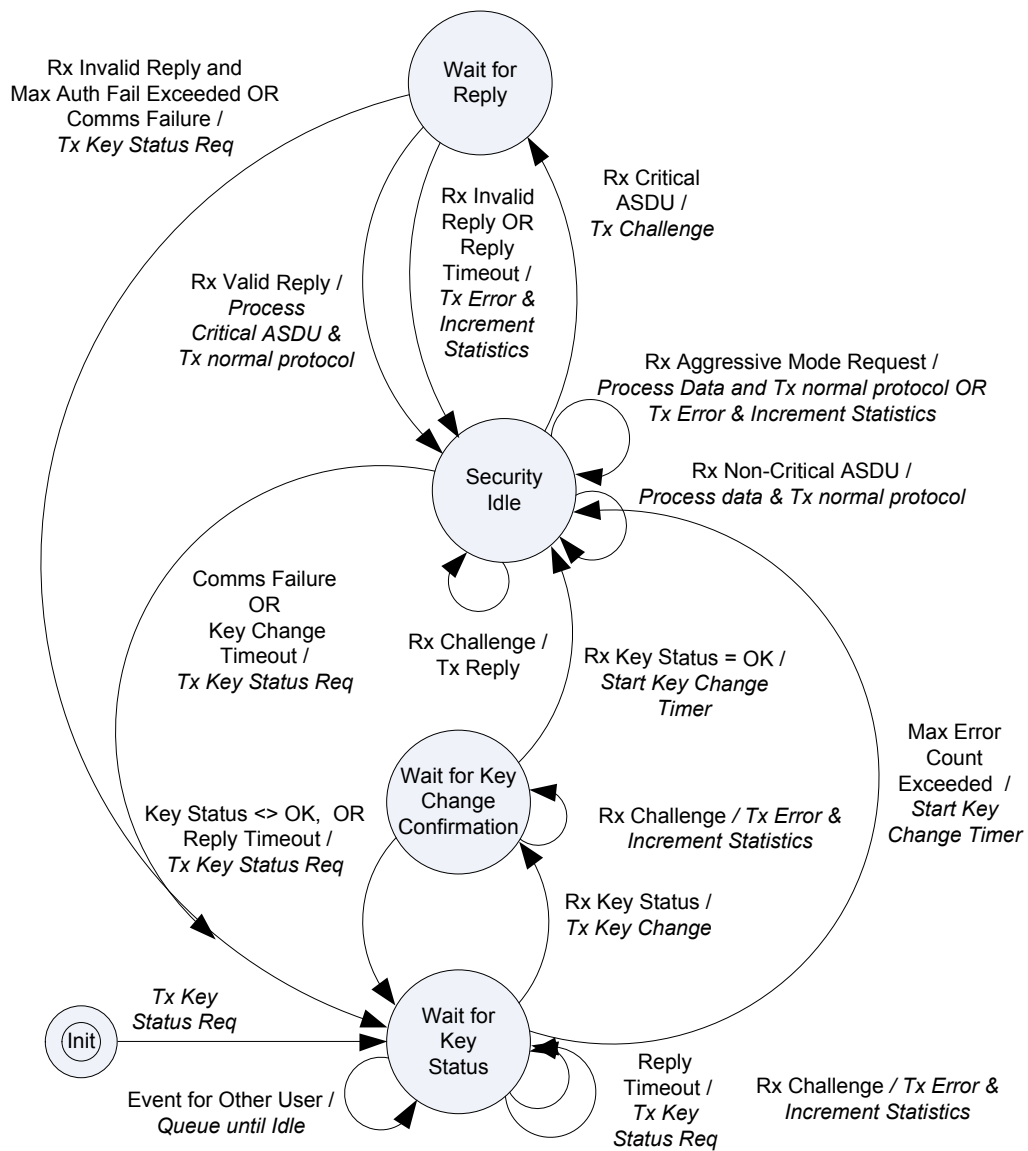
6.4 State machine overview

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.



IEC 703/13

Figure 10 – Major state transitions for controlling station authentication

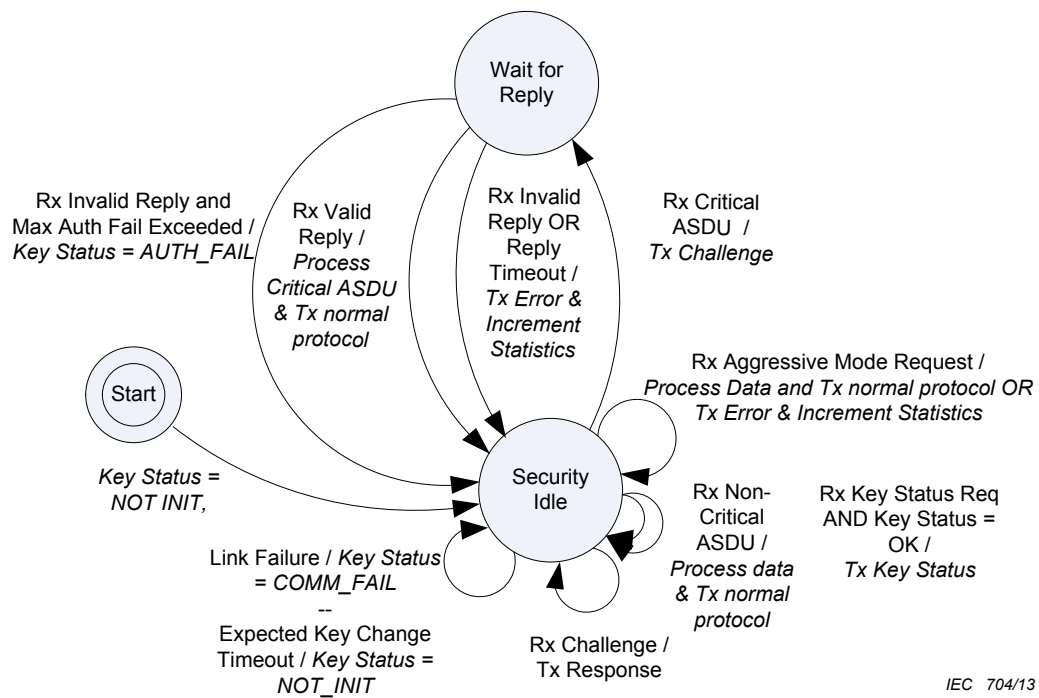
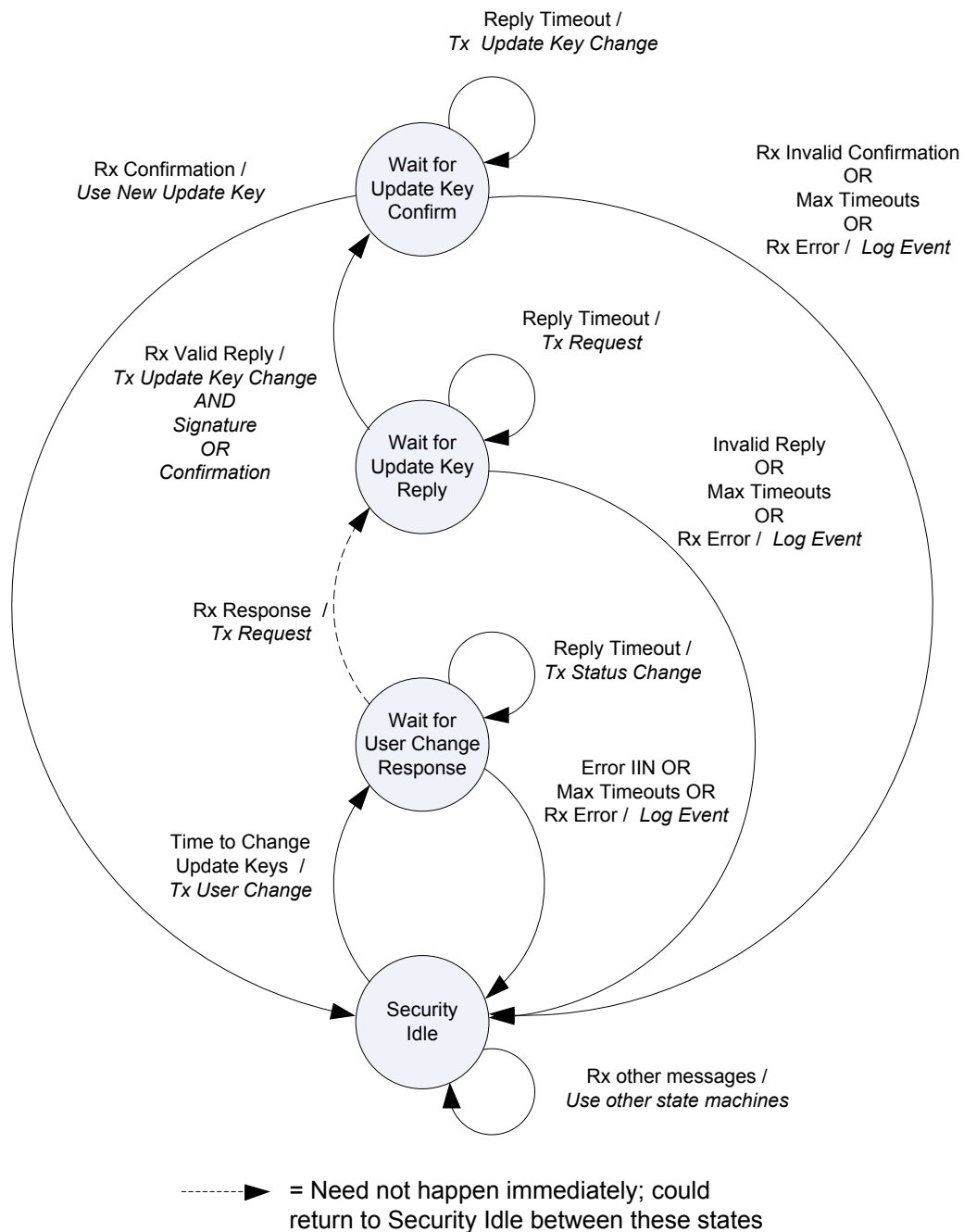
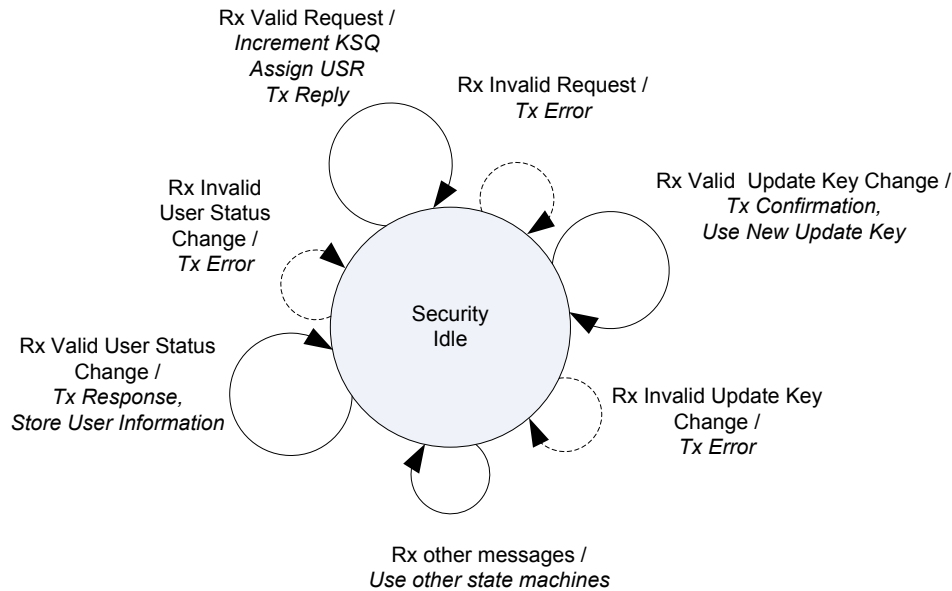


Figure 11 – Major state transitions for controlled station authentication



IEC 705/13

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



-----► = Do not transmit Error if Max Error Count is exceeded

IEC 706/13

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 <i>previous</i> 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
------------	------------------------