

TECHNICAL SPECIFICATION

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00



IEC/TS 62351-5

Edition 1.0 2009-08

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 **XA**

ICS 33.200

ISBN 978-2-88910-681-3

CONTENTS

FOREWORD.....	6
1 Scope and object.....	8
1.1 Scope.....	8
1.2 Intended audience and use	8
1.3 Items outside of scope	8
1.4 Use with other standards.....	8
1.5 Document organization and approach.....	9
1.6 Compliance	9
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	11
5 Problem description.....	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	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	17
6.2.5	Authentication failure.....	18
6.2.6	Aggressive mode	18
6.2.7	Changing keys.....	18
6.3	Example message sequences	19
6.3.1	Overview of subclause.....	19
6.3.2	Challenge of a critical ASDU	20
6.3.3	Aggressive mode	21
6.3.4	Initializing and changing session keys	22
6.4	State machine overview	23
7	Formal specification	25
7.1	Overview of clause	25
7.2	Message definitions.....	25
7.2.1	Distinction between messages and ASDUs.....	25
7.2.2	Challenge message	25
7.2.3	Reply message.....	27
7.2.4	Aggressive mode request	29
7.2.5	Key status request message.....	31
7.2.6	Key status message	31
7.2.7	Session key change message.....	34
7.2.8	Error message	36
7.3	Formal procedures	38
7.3.1	Overview of subclause.....	38
7.3.2	Challenger procedures	38
7.3.3	Responder procedures	48
7.3.4	Controlling station procedures	48
7.3.5	Controlled station procedures	53
8	Interoperability requirements	53
8.1	Overview of clause	53
8.2	Minimum requirements	53
8.2.1	Overview of subclause.....	53
8.2.2	HMAC algorithms	53
8.2.3	Key wrap algorithms	54
8.2.4	Fixed values	54
8.2.5	Configurable values	54
8.3	Options	55
8.3.1	Overview of subclause.....	55
8.3.2	HMAC algorithms	55
8.3.3	Encryption algorithms	55
8.3.4	Configurable values.....	56
9	Special applications.....	56
9.1	Overview of clause	56
9.2	Use with TCP/IP	56
9.3	Use with redundant channels.....	56

9.4	Use with external link encryptors	56
10	Requirements for referencing this specification.....	57
10.1	Overview of clause	57
10.2	Selected options.....	57
10.3	Operations considered critical	57
10.4	Addressing information.....	57
10.5	Message format mapping	57
10.6	Reference to procedures	57
11	Protocol implementation conformance statement.....	58
11.1	Overview of clause	58
11.2	Required algorithms	58
11.3	HMAC algorithms	58
11.4	Key wrap algorithms.....	58
11.5	Maximum error count.....	58
11.6	Use of error messages	58
	Bibliography.....	59
	Figure 1 – Example of successful challenge of critical ASDU	20
	Figure 2 – Example of failed challenge of critical ASDU.....	20
	Figure 3 – Example of a successful aggressive mode request.....	21
	Figure 4 – Example of a failed aggressive mode request	21
	Figure 5 – Example of session key initialization and periodic update.....	22
	Figure 6 – Example of communications failure followed by session key change	23
	Figure 7 – Major state transitions for controlling station	24
	Figure 8 – Major state transitions for controlled station	25
	Table 1 – Scope of application to standards.....	8
	Table 2 – Summary of keys used	18
	Table 3 – Challenge message.....	26
	Table 4 – Reply message	28
	Table 5 – Data included in the HMAC value calculation.....	29
	Table 6 – Aggressive mode request message	29
	Table 7 – Data included in the HMAC value calculation in aggressive mode	30
	Table 8 – Key status request message	31
	Table 9 – Use of default session keys.....	31
	Table 10 – Key status message	32
	Table 11 – Data included in the HMAC value calculation for key status.....	34
	Table 12 – Key change message	34
	Table 13 – Data included in the key wrap (in order)	35
	Table 14 – Example of key order.....	35
	Table 15 – Example of wrapped key data.....	36
	Table 16 – Error message.....	36

Table 17 – States used in the state machine descriptions	38
Table 18 – Challenger state machine	41
Table 19 – Controlling station state machine.....	50

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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 62351-5, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/861/DTS	57/921A/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.

A list of all parts of the IEC 62351 series, 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 maintenance result 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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

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

Part 5: Security for IEC 60870-5 and derivatives

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures and algorithms for securing the operation of all protocols based on or derived from the standard IEC 60870-5: Telecontrol equipment and systems – Part 5: Transmission protocols. This 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	Companions 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)

1.2 Intended audience and use

The initial audience for this 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.

1.3 Items outside of scope

This part of IEC 62351 focuses only on application layer authentication and security issues arising from such authentication, per directions from IEC Technical Committee 57 Working Group 3. 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.

1.4 Use with other standards

The working groups developing the protocols listed in Table 1 may issue standards to be applied in conjunction with this specification. It is expected that these standards will describe a mapping of this authentication mechanism to the messages and procedures of each specific protocol.

Such documents shall not override any of the security measures described in this specification as mandatory and normative.

When applied to IEC 60870-5-104, this specification shall be applied in conjunction with 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.

1.5 Document organization and approach

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.

1.6 Compliance

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

2 Normative references

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

IEC 60870-5-101, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

IEC 60870-5-102, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems*

IEC 60870-5-103, *Telecontrol equipment and systems – Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment*

IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

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*

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

FIPS 186-2, *Digital Signature Standard (DSS)*

FIPS 197, *Advanced Encryption Standard (AES)*

FIPS 198-1, *The Keyed-Hash Message Authentication Code*

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

RFC 3174, *Secure Hash Algorithm (SHA-1)*

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

They are described here because they are specific to the IEC 60870-5 standards and may be useful for reading this specification as an independent document.

Refer to IEC/TS 62351-2 for a list of applicable terms and definitions.

3.1

controlling station

the device or application that initiates most of the communications and issues commands

It is commonly called a “master” in some protocol specifications.

3.2

controlled station

the remote device that transmits data gathered in the field to the controlling station

It is commonly called the “outstation” or “slave” in some protocols.

3.3

control direction

data transmitted by the controlling station to the controlled station(s)

3.4

monitoring direction

data transmitted by the controlled station to the controlling stations

The following terms are described here because they are specific to this protocol:

3.5

challenger

station that issues authentication challenges

It may be either a controlled or controlling station.

3.6

responder

station that responds or reacts to authentication challenges

It may be either a controlled or controlling station.

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

5.1 Overview of clause

This clause is informative only. It 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;
- non-repudiation – to the extent of identifying individual users of the system.

5.3 Design issues

5.3.1 Overview of subclause

This subclause describes the challenges faced in developing an authentication proposal that can be applied to all the IEC 60870-5 and derivative protocols. This subclause 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

This subclause 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 in 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 does not prevent the use of public-key cryptography or other key distribution mechanisms to be used to change or distribute the pre-shared keys described here. Future specifications may standardize such methods, but they are currently out of the scope of this specification.

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

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 in audit logs for non-repudiation purposes, although such use is out of the scope 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. However, this document does not specify a mechanism for such user-based or role-based access control.

6 Theory of operation (informative)

6.1 Overview of clause

This clause describes the operation of the authentication mechanism in general terms for the benefit of first-time readers. This clause 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 1. Because “response” is a keyword in the affected protocols, the term used here is “reply”;
- the concept of a keyed-hash message authentication code (HMAC) 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 HMAC 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 HMAC 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 HMAC output.
- It is nearly impossible to determine the original message from the HMAC.
- It is difficult to find two messages that produce the same HMAC.

This challenge-reply mechanism using an HMAC 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 7.3.2.2. 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 cryptographic keyed-hash message authentication code (HMAC) 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 HMAC 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 HMAC 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 perform the requested operation. The challenger may then choose to transmit an error message. To help protect against denial-of-service attacks, the challenger shall cease to transmit error messages after a fixed number of failures. The controlling station must reset the session keys before the error condition can be cleared.

6.2.6 Aggressive mode

To reduce bandwidth usage, a responder attempting a critical operation may optionally “anticipate” the challenge and send the HMAC value in the same ASDU being protected. This eliminates the challenge and reply messages. Aggressive mode provides a lower level of security, because not as much data is changing in each message.

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 summarizes how cryptographic keys are used and updated in this authentication mechanism. 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.

Table 2 – Summary of 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 shall be pre-shared by the two devices and is changed only by means external to the protocol.	Months or years

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.