



BSI Standards Publication

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

Part 5: Security for IEC 60870-5 and derivatives

National foreword

This British Standard is the UK implementation of EN 62351-5:2023. It is identical to IEC 62351-5:2023. It supersedes PD IEC/TS 62351-5:2013, which will be withdrawn on 3 July 2023.

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 committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 05925 0

ICS 33.200

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2023.

Amendments/corrigenda issued since publication

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

English Version

Power systems management and associated information
exchange - Data and communications security - Part 5: Security
for IEC 60870-5 and derivatives
(IEC 62351-5:2023)

Gestion des systèmes de puissance et échanges
d'informations associées - Sécurité des communications et
des données - Partie 5: Aspects de sécurité pour l'IEC
60870-5 et ses dérivés
(IEC 62351-5:2023)

Energiemanagementsysteme und zugehöriger
Datenaustausch - IT-Sicherheit für Daten und
Kommunikation - Teil 5: Sicherheit für IEC 60870-5 und
Derivate
(IEC 62351-5:2023)

This European Standard was approved by CENELEC on 2023-02-17. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 57/2516/FDIS, future edition 1 of IEC 62351-5, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62351-5:2023.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2023-08-17
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2026-02-17

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

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62351-5:2023 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 60870-5-101:2003 NOTE Approved as EN 60870-5-101:2003 (not modified)

IEC 60870-5-102 NOTE Approved as EN 60870-5-102

IEC 60870-5-103 NOTE Approved as EN 60870-5-103

IEC 60870-5-104 NOTE Approved as EN 60870-5-104

Annex A (normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60870-5	series	Telecontrol equipment and systems – Part 5: Transmission protocols	EN 60870-5	series
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 62351-3	-	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP	EN 62351-3	-
IEC 62351-7	-	Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models	EN 62351-7	-
IEC 62351-8	-	Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management	EN IEC 62351-8	-
IEC 62351-14 ¹	-	Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging	-	-

¹ Under preparation. Stage at the time of publication: IEC ACDV 62351-14:2021.

EN IEC 62351-5:2023 (E)

IETF RFC 2104	-	HMAC: Keyed-Hashing for Message Authentication	-	-
IETF RFC 3394	-	Advanced Encryption Standard (AES) Key Wrap Algorithm	-	-
IETF RFC 5116	-	An Interface and Algorithms for Authenticated Encryption	-	-
IETF RFC 5869	-	HMAC-based Extract-and-Expand Key Derivation Function	-	-
IETF RFC 7693	-	The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)	-	-
IETF RFC 7748	-	Elliptic Curves for Security	-	-
SEC2-V2	-	Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain parameters - Version 2.0	-	-

CONTENTS

FOREWORD.....	6
1 Scope.....	8
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	11
5 Problem description.....	12
5.1 Overview of clause	12
5.2 Specific threats addressed.....	12
5.3 Design issues	12
5.3.1 Overview of subclause.....	12
5.3.2 Asymmetric communications.....	12
5.3.3 Message-oriented	12
5.3.4 Poor sequence numbers or no sequence numbers.....	13
5.3.5 Limited processing power	13
5.3.6 Limited bandwidth.....	13
5.3.7 No access to authentication server	13
5.3.8 Limited frame length	13
5.3.9 Limited checksum	14
5.3.10 Radio systems	14
5.3.11 Dial-up systems	14
5.3.12 Variety of protocols affected	14
5.3.13 Differing data link layers	14
5.3.14 Long upgrade intervals	15
5.3.15 Remote sites	15
5.3.16 Unreliable media	15
5.4 General principles.....	15
5.4.1 Overview of subclause.....	15
5.4.2 Application layer only	15
5.4.3 Generic definition mapped onto different protocols	15
5.4.4 Bi-directional	15
5.4.5 Management of cryptographic keys.....	15
5.4.6 Backwards tolerance	16
5.4.7 Upgradeable.....	16
5.4.8 Multiple connections	16
6 Theory of operation	16
6.1 Overview of clause	16
6.2 The secure communication	16
6.2.1 Basic concepts	16
6.2.2 Association ID	17
6.2.3 Authenticating	18
6.2.4 Central Authority.....	18
6.2.5 Role Based Access Control (RBAC).....	18
6.2.6 Cryptographic keys	18
6.2.7 Security statistics	22
6.2.8 Security events.....	22
7 Functional requirements	22

7.1	Overview of clause	22
7.2	Procedures Overview.....	22
7.3	State machine overview	23
7.4	Timers and counters	25
7.5	Security statistics and events.....	25
7.5.1	General	25
7.5.2	Special security thresholds	29
7.5.3	Security statistics reporting.....	29
7.5.4	Security events monitoring and logging	29
8	Formal procedures	30
8.1	Overview of subclause	30
8.2	Distinction between messages and ASDUs	30
8.2.1	General	30
8.2.2	Messages datatypes and notations	30
8.3	Station Association procedure.....	30
8.3.1	General	30
8.3.2	Public key certificates	31
8.3.3	Configuration of authorized remote stations	33
8.3.4	Pre-requisites to initiate the Station Association procedure.....	33
8.3.5	Messages definition	33
8.3.6	Controlling station state machine	42
8.3.7	Controlled station state machine	52
8.3.8	Verification of remote station's certificate	61
8.3.9	Verification of certificates during normal operations	61
8.3.10	Update Keys derivation	62
8.3.11	Controlling station directives for Station Association and Update Keys management.....	63
8.3.12	Controlled station directives for Station Association and Update Keys management.....	63
8.3.13	Initializing and updating Stations Association and Update Keys	65
8.4	Session Key Change procedure	66
8.4.1	General	66
8.4.2	Messages definition	67
8.4.3	Controlling station state machine	76
8.4.4	Controlled station state machine	85
8.4.5	Controlling station directives for Session Keys management.....	93
8.4.6	Controlled station directives for Session Keys management	93
8.4.7	Initializing and changing Session Keys	94
8.5	Secure Data Exchange	95
8.5.1	General	95
8.5.2	Messages definition	96
8.5.3	Controlling station state machine	100
8.5.4	Controlled station state machine	105
8.5.5	Controlling station directives for Secure Data Exchange	109
8.5.6	Controlled station directives for Secure Data Exchange	109
8.5.7	Example of Secure Data exchange during Station Association.....	110
8.5.8	Example of Secure Data Exchange during Session Key Change.....	111
9	Interoperability requirements	113
9.1	Overview of clause	113

9.2	Minimum requirements	113
9.2.1	Overview of subclause	113
9.2.2	Authentication algorithms	113
9.2.3	Key wrap / transport algorithms	113
9.2.4	Cryptographic keys	114
9.2.5	Cryptographic curves	114
9.2.6	Configurable values	114
9.2.7	Cryptographic information	116
9.3	Options	116
9.3.1	Overview of subclause	116
9.3.2	MAC/AEAD algorithms	117
9.3.3	Key wrap / transport algorithms	117
9.3.4	Cryptographic curves	117
9.4	Use with TCP/IP	117
9.5	Use with redundant channels	117
10	Requirements for referencing this standard	118
10.1	Overview of clause	118
10.2	Selected options	118
10.3	Message format mapping	118
10.4	Reference to procedures	118
10.5	Protocol information	118
10.6	Controlled station response to unauthorized operations requests	119
10.7	Transmission of security statistics	119
10.8	Configurable values	119
10.9	Protocol implementation conformance statement	119
Annex A (informative)	Security Event mapping to IEC 62351-14	120
A.1	General	120
A.2	Mapping of IEC 62351-5 events specified in this document	120
Bibliography		122
Figure 1	– Overview of interaction between Central Authority and stations	21
Figure 2	– Sequence of procedures	23
Figure 3	– Station Association procedure	34
Figure 4	– Station Association – Controlling station state machine	43
Figure 5	– Station Association – Controlled station state machine	53
Figure 6	– Example of Association ID, Update Keys and Session Keys initialization	66
Figure 7	– Session Key Change procedure	67
Figure 8	– Session Key Change – Controlling station state machine	77
Figure 9	– Session Key Change – Controlled station state machine	86
Figure 10	– Example of Session Key initialization and periodic update	95
Figure 11	– Secure Data Exchange	96
Figure 12	– Secure Data Exchange – Controlling station state machine	101
Figure 13	– Secure Data Exchange – Controlled station state machine	106
Figure 14	– Example of Secure Data Exchange during Station Association	111
Figure 15	– Example of Secure Data messages exchanged during Session Key Change	112

Table 1 – Scope of application to standards.....	8
Table 2 – Summary of symmetric keys used	19
Table 3 – Summary of asymmetric keys used	19
Table 4 – States used in the controlling station state machine	24
Table 5 – States used in the controlled station state machine	24
Table 6 – Summary of timers and counters used.....	25
Table 7 – Security statistics and associated events	26
Table 8 – Elliptic curves.....	31
Table 9 – Association Request message.....	35
Table 10 – Association Response message	36
Table 11 – Update Key Change Request message.....	38
Table 12 – Data Included in MAC calculation (in order).....	40
Table 13 – Update Key Change Response message	40
Table 14 – Data Included in MAC calculation (in order).....	41
Table 15 – Controlling station state machine: Station Association	44
Table 16 – Controlled station state machine: Station Association	54
Table 17 – List of pre-defined role-to-permission assignment.....	64
Table 18 – Session Request message	68
Table 19 – Session Response message.....	70
Table 20 – Data Included in MAC calculation (in order).....	71
Table 20 – Session Key Change Request message	72
Table 21 – Data Included in WKD (in order)	73
Table 22 – Example of Session Key order.....	74
Table 23 – Data Included in the MAC calculation (in order)	74
Table 25 – Session Key Change Response message.....	75
Table 26 – Data Included in the MAC calculation (in order)	75
Table 27 – Controlling station state machine: Session Key Change	78
Table 28 – Controlled station state machine: Session Key Change	87
Table 29 – Secure Data message	97
Table 29 – Secure Data Payload using MAC algorithm	98
Table 31 – Data included in the MAC calculation in Secure Data Payload (in order).....	99
Table 32 – AEAD algorithm parameters to generate the Secure Data Payload (in order).....	99
Table 33 – Controlling station state machine: Secure Data Exchange	102
Table 34 – Controlled station state machine: Secure Data Exchange	107
Table 35 – Configuration of cryptographic information	116
Table 36 – Legend for configuration of cryptographic information.....	116
Table A.1 – Security event logs defined in IEC 62351-5 Ed.1 mapped to IEC 62351-14	120

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.

IEC 62351-5 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is an International Standard.

This International Standard cancels and replaces IEC TS 62351-5 published in 2013. It constitutes a technical revision. The primary changes in this International Standard are:

- a) The secure communication mechanism is performed on per controlling station/controlled station association.
- b) User management to add, change or delete a User, was removed.
- c) Symmetric method to change the Update Key was removed.
- d) Asymmetric method to the change Update Key was reviewed.
- e) Challenge/Reply procedure and concepts were removed.
- f) Aggressive Mode concept was replaced with the Secure Data message exchange mechanism.
- g) Authenticated encryption of application data was added.

- h) The list of permitted security algorithms has been updated.
- i) The rules for calculating messages sequence numbers have been updated
- j) Events monitoring and logging was added.

NOTE The following print types are used:

CAPITALIZATION has been used in the text of this document 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) procedure names, e.g. Station Association, Session Key Change; message names, e.g. Association Request, Session Request; 3) state names, e.g. Session Established, Wait for Session Response; 5) statistics e.g. Authentication Errors, Unexpected Messages and 5) event names e.g. Reply Timeout, Rx Invalid Session Key Change.

The text of this International Standard is based on the following documents:

Draft	Report on voting
57/2516/FDIS	57/2555/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

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

This part of IEC 62351 defines the application profile (A-profile) secure communication mechanism specifying 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 document 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 (defined in IEEE Std 1815, based on IEC 60870-1 through IEC 60870-5 and maintained jointly by the DNP Users Group and the IEEE)

The initial audience for this document is intended to be the members of the working groups developing the protocols listed in Table 1.

For the measures described in this document 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 working groups in charge of taking this document to the specific protocols listed in Table 1 may choose not to do so.

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

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

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 define the interoperability requirements for this secure communication mechanism, including the relationship of this standard to IEC 62351-3 for transport layer security..
- Clause 10 describes the requirements for other standards referencing this document.

The actions of an organization in response to events and error conditions described in this document are expected to be defined by the organization's security policy and they are beyond the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 (all parts), *Telecontrol equipment and systems – Part 5: 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 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 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

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

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging*¹

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

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

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption*

IETF RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

IETF RFC 7693, *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*

IETF RFC 7748, *Elliptic Curve for Security*

SEC2-V2, *Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain Parameters – Version 2.0*

¹ Under preparation. Stage at the time of publication: IEC ACDV 62351-14:2021.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

association ID

pair of values that uniquely identify the communication link between a controlling station and a controlled station and the related set of cryptographic keys

3.2

central authority

entity whose scope is the entire organization for which the purpose is to provide authentication information to devices and systems of the organization to authorize them to communicate. The Central Authority may or may not also be a Certificate Authority

3.3

communication link

the communication channel that connects two communicating entities. This link may be an actual physical link or it may be a logical link that uses one or more actual physical links.

3.4

control direction

direction of transmission from the controlling station to a controlled station

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

3.5

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 TR 60870-1-3:1997, 3, modified (addition of "(controlling" and Note 1 to entry)]

3.6

controlling station

station which performs the telecontrol of controlled stations

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

[SOURCE: IEC TR 60870-1-3:1997, 3, modified (replacement of "outstations" with "controlled stations)]

3.7

local station

station nearest to the observer when the process is the same on both the controlling and controlled station

3.8

monitoring direction

direction of transmission from a controlled station to a controlling station

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

3.9**remote station**

station farther from the observer when the process is the same on both the controlling and controlled station

3.10**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 TR 60870-1-3:1997, 3]

4 Abbreviated terms

Refer to IEC TS 62351-2 for a list of applicable abbreviated terms. The following terms are included here because they are specifically used in the affected protocols and also used in the discussion of this secure communication mechanism.

A-Profile	Application Profile. Security for the application layer.
AEAD	Authenticated Encryption with Associated Data. Function to encrypt and authenticate data (providing confidentiality and authentication). Note that AEAD also supports integrity protection of additional data, which is not encrypted.
AID	Association ID. Value identifying a single connection between controlling and Controlled stations.
ASDU	Application Service Data Unit. The application layer message submitted to lower layers for transmission.
C.ing	Controlling (referred to the controlling Station).
C.led	Controlled (referred to the controlled Station).
HKDF	HMAC-based Extract-and-Expand Key Derivation Function. Function to derive a symmetric cryptographic key.
HMAC	Keyed-Hash Message Authentication Code. Function to authenticate data using a secret cryptographic key.
IKM	Input Keying Material. Data provided to the HKDF-Extract function to generate a pseudo-random key (PRK).
KEK	Key Encryption Key. A secret key used to encrypt another secret key.
MAC	Message Authentication Code. The calculated value used by a station to authenticate and check the integrity of an Application Protocol Data Unit.
PRK	Pseudo-Random Key. Data provided to the HKDF-Expand function to generate a secret key.
T-Profile	Transport Profile. Security for transport layer (TCP/IP)
TCP/IP	Transmission Control Protocol/Internet Protocol.

5 Problem description

5.1 Overview of clause

Clause 5 describes:

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

5.2 Specific threats addressed

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

- spoofing;
- tampering;
- replay;
- eavesdropping

5.3 Design issues

5.3.1 Overview of subclause

Subclause 5.3 describes the challenges faced in developing a secure communication proposal that can be applied to all the IEC 60870-5 and derived 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 secure communication mechanism:

- the format of messages in each direction will almost certainly differ, even if the functions are the same;
- Session 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. Connection authentication is done once to establish session keys, which in turn are used afterwards to support message authentication.

Message 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 secure communication 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 communication links also charge costs per octet transmitted.

Therefore, the secure communication mechanism must not add very much overhead (i.e. few octets) to the affected protocols. The size of the additional 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 secure communication 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 secure communication 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, except that there is no check for the entire frame.

Therefore, the secure communication mechanism described in this standard 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 standard 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 security extension described in this standard always uses a method to authenticate all application data messages, 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 secure communication 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 secure communication 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 secure communication mechanism follows the principles described in 5.4.

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 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 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 document, based on the identified threats and design issues discussed in the previous two clauses.

5.4.2 Application layer only

This document describes the secure communication as an A-Profile. Refer to IEC 62351-1 for a discussion of why application-to-application security is necessary in the utility environment, in addition to any transport layer security that may be implemented.

5.4.3 Generic definition mapped onto different protocols

This document describes a common method of encryption and 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 document according to the rules defined in Clause 10.

5.4.4 Bi-directional

This document 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.

5.4.5 Management of cryptographic keys

This document provides the method to remotely change keys using a combination of asymmetric (public-key) and symmetric cryptography to manage security credentials.

This document uses multiple levels of keys for the following reasons:

- A symmetric periodically changed Session Keys is used to protect against brute force attack and limits computational power required.
- A symmetric infrequently changed Update Keys is used to renew the Session Keys.
- An asymmetric key pair owned by each device is used to change the Update Keys because it easier to manage and distribute them in certificates.

5.4.6 Backwards tolerance

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

- The secure device should be able to detect that the non-secure device does not support the secure communication 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.

5.4.7 Upgradeable

This document permits system administrators to change algorithms and other security parameters to deal with future requirements. In keeping with the principle of interoperability between devices, it also permits one end of a link to be upgraded at a time.

5.4.8 Multiple connections

This document assumes that there may be multiple controlling stations connected to the same controlled station and communicating simultaneously. It provides a method to identify and authenticate each of the controlling stations connected, separately from each other, regardless their address information.

The Association ID discussed in this document permits to identify each communication link in the system as controlling/controlled stations association. It also allows for the possibility that controlled stations may limit access to certain functions based on "roles" and "right" (RBAC) assigned to the controlling station.

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 Errors 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 communication link. For the best forensic results, stations should log entire messages, including all authentication information, so an auditor can evaluate the authenticity of the messages.

6 Theory of operation

6.1 Overview of clause

Clause 6 describes the operation of the secure communication mechanism in general terms for the benefit of first-time readers. In the case of discrepancies between this clause and Clause 7, Clause 7 shall be taken as correct.

6.2 The secure communication

6.2.1 Basic concepts

6.2.1.1 Overview

The secure communication defined in this document is based on the authentication and the optional encryption of the data transmitted over the communication link by using cryptographic keys.

6.2.1.2 Authentication-only mode

When using the authentication-only mode, the secure communication mechanism is based on the concept of a Message Authentication Code (MAC) that both the controlled and controlling stations calculate for each Application Service Data Unit (ASDU, or protocol message) that is to be authenticated.

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

- The MAC function takes as inputs the key and the protocol message and outputs the authentication tag.
- 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 message and 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.

6.2.1.3 Authenticated encryption mode

When using an authenticated-and-encrypted mode, the secure communication mechanism is based on the concept of authenticated encryption with additional data (AEAD). This is a form of encryption that simultaneously ensures the confidentiality and the authenticity of the data, using a symmetric encryption key and an authentication tag. The authentication tag can further include information from additional data which may be sent as plain text (and is therefore not confidential).

An AEAD has the following characteristics:

- The inputs of the encryption function are the plaintext to be encrypted, the plaintext to be used as additional data, a symmetric key, and a nonce.
- The outputs of the encryption function are the ciphertext and an authentication tag.
- The inputs of the decryption function are the symmetric key, the nonce, the additional data, the ciphertext and the authentication tag.
- The outputs of the decryption function are a Boolean value indicating whether authentication was successful, and the plaintext originally input into the encryption function (provided authentication was successful).
- The authentication tag, like a MAC, is extremely sensitive to slight changes in the input, so it can be used to detect if the message (including the cleartext additional data) was modified.
- It is extremely difficult to determine either the secret key or the plaintext from the function's output.
- It is extremely difficult to find two messages that produce the same authentication tag.

6.2.2 Association ID

In this secure communication mechanism, each communication link is identified by a numeric Association ID. The Association ID is composed of the controlling station Association ID and the controlled station Association ID concatenated. Each association has its corresponding set of cryptographic keys used to encrypt and/or authenticate the information exchanged. The cryptographic keys are described in 6.2.6.

6.2.3 Authenticating

Upon receiving a message containing authentication information, the receiver performs the same calculation on the same data used by the sender. If the results match, the receiver permits communications to continue. If the sender was protecting a particular ASDU (application data), the receiver shall process that ASDU.

If the authentication fails, the receiver does not use data from the message received and the message shall be discarded. If the receiver is a controlled station, it does not perform the operation requested in the message.

6.2.4 Central Authority

No particular user of a controlling station should be trusted with the capability to add or remove a station in the system. That function should be performed by authorized personnel or by a Central Authority whose scope is the entire organization. The Central Authority may or may not also be a Certificate Authority. The specification of the full functionality of the Central Authority is not in scope of this document.

6.2.5 Role Based Access Control (RBAC)

In this secure communication mechanism, one or more specific roles can be assigned to the controlling station according to IEC 62351-8. Each role has a specific set of operations permitted on the controlled station. The controlled station verifies that the role assigned to the controlling station permits the controlling station to perform the operation requested.

Assignment of roles to the controlling station must be performed by authorized personnel or by the Central Authority.

6.2.6 Cryptographic keys

6.2.6.1 General

Table 2 and Table 3 summarize how cryptographic keys are used and updated in this secure communication mechanism. At a minimum, keys are managed by the controlled station and controlling station. Optionally, a trusted third party known as the Central Authority may manage certificates and policies used for key management.

Table 2 – Summary of symmetric keys used

Type	Use	Change mechanism	Range of expected change interval
Monitoring Direction Session Key	Used to authenticate and optionally encrypt the data transmitted in the monitoring direction by the controlled station.	The controlling station wraps the Monitoring Direction and Control Direction Session Keys using the Encryption Update Key and transmits the wrapped Session Keys in a Session Key Change message authenticated with the Authentication Update Key.	Minutes to weeks
Control Direction Session Key	Used to authenticate and optionally encrypt the data transmitted in the control direction by the controlling station.	The controlling station wraps the Monitoring Direction and Control Direction Session Keys using the Encryption Update Key and transmits the wrapped Session Keys in a Session Key Change message authenticated with the Authentication Update Key.	Minutes to weeks
Authentication Update Key	Symmetric key used by both the controlling station and the controlled station to authenticate the Encryption Update Key and the Session Keys when they are periodically changed.	The Authentication Update Key is generated and agreed by the two stations using an Elliptic Curve Diffie-Hellmann exchange (ECDH) and an HMAC-based Extract-and-Expand Key Derivation Function (HKDF).	Months or Years
Encryption Update Key	Symmetric key used by the controlling station and the controlled station respectively to wrap and unwrap the Session Keys when they are periodically changed.	The Encryption Update Key is generated and agreed by the two stations using an Elliptic Curve Diffie-Hellmann exchange (ECDH) and an HMAC-based Extract-and-Expand Key Derivation Function (HKDF).	Months or Years

Table 3 – Summary of asymmetric keys used

Type	Use	Change mechanism	Range of expected change interval
Central Authority Private Key	The Central Authority acting as Certificate Authority uses its Private Key to certify the Public Key of a device.	The Central Authority's Private Key is kept secret by the Central Authority and may only be changed by means external to the protocol.	Years, if ever
Central Authority Public Key	The local station uses the Central Authority's Public Key to validate the Public Key certificate of the remote station.	The Central Authority's Public Key is contained in a Public Key Certificate. It may be transmitted anywhere in the clear but must be securely installed in the controlling station and in the controlled station by trusted personnel.	Years, if ever
Station Private Key	The local station uses its Private Key to perform the Update Keys agreement with the remote station	The station's Private Key should be generated by the station itself and stored securely on the device, or it must be installed and stored securely in the station by trusted personnel	Years if ever
Station Public Key	The local station uses the remote station's Public Key to perform the Update Keys agreement with the remote station.	The station's Public Key should be generated by the station itself and is contained in a Public Key Certificate which may be transmitted anywhere in the clear. If the public/private key pair and the certificate is generated by a Central Authority it must be installed and stored securely in the station by trusted personnel.	Years if ever

6.2.6.2 Session Keys

The Session Keys are the most frequently used keys. Each station uses the Session Keys to authenticate or encrypt-and-authenticate the application data sent and received.

There are two different Session Keys, one used for authenticating data in the monitoring direction, and one for authenticating data transmitted in the control direction, so that if the key used for one direction is compromised, it does not compromise communications in the other direction.

There is a different set of Session Keys for each controlling station/controlled station Association, identified by the Association ID.

The Session Keys of an Association can be initialized and changed thereafter only if the Update Keys have been previously initialized for the same Association by performing the Station Association procedure, described in 8.3.

The controlling station initializes the Session Keys immediately after communications is established if the Session Keys are not valid and changes the Session Keys thereafter on regular basis. This practice of periodically changing the Session Keys protects them from being compromised through analysis of the communications link.

The Session Keys are periodically changed performing the Session Key Change procedure described in 8.4. In this procedure the Session Keys are wrapped and authenticated by the controlling station using the Update Keys and transmitted to the controlled station. The use of a second key pair, the Update Keys, permits the controlling station to change the Session Keys even if the original Session Keys were compromised. Both the Session Keys and the Update Keys are symmetric keys.

It is vital for security that each device keeps Session Keys secret. The mechanism used to do so is out of the scope of this document, but implementers should note that if Session Keys are stored on the device in an insecure fashion, the entire secure communication mechanism is compromised.

Note that if Session Keys are stored in non-volatile storage, devices shall ensure that the same sequence numbers in the messages are not re-used with the same Session Keys and that the Session Key expiry due to use time-out or use count are still respected.

6.2.6.3 Update Keys

The Update Keys are symmetric keys:

- the Encryption Update Key is a Key Encryption Key (KEK) used to wrap the Session Keys on the controlling station and unwrap the Session Keys on the controlled station
- the Authentication Update Key is used to authenticate the Station Association procedure described in 8.3 and the Session Key Change procedure described in 8.4.

There is a different set of Update Keys for each controlling station/controlled station Association. For each Association, the controlling station may be assigned to a Role designating specific actions it is permitted to perform.

The Update Keys for each Association ID are initialized and changed by performing the Station Association procedure described in 8.3.

The Update Keys agreement between the controlling station and the controlled station is performed at the first time during the station enrolment phase after the station installation or replacement.

The Update Keys are rarely changed. The reason for such a change is dependent on the security policy of the organization, but may include the Update Keys being compromised, or when the controlling station's Role changes. The method used to agree the Update Keys is based on the asymmetric (public key) cryptography.

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 document, but implementers should note that if Update Keys are stored on the device in an insecure fashion, the entire secure communication mechanism is compromised.

The Update Keys agreed during Station Association procedure shall be stored permanently on each station, so that this procedure shall not be executed after a station initialization or after a communication failure.

6.2.6.4 Station's public and private keys.

The station's public and private keys are used to agree on the Update Keys. To this end, controlling station and controlled station exchange their public key. This method requires the use of public key certificates. The certificate is provisioned to the station when the station is to be added or replaced in the system or that its Role should be changed.

In general, as shown in Figure 1, the station's job (either controlling or controlled) is merely to forward its public key certificate to the other station connected and authorized to communicate, and to ensure that the new Update Keys assigned to the corresponding controlling station/controlled station association are agreed in a secure fashion.

The communications between the station and the Central Authority for the purpose of certifying the station itself is out of the scope of this document but must also be secure. Further information on certificate management may be found in IEC 62351-9.

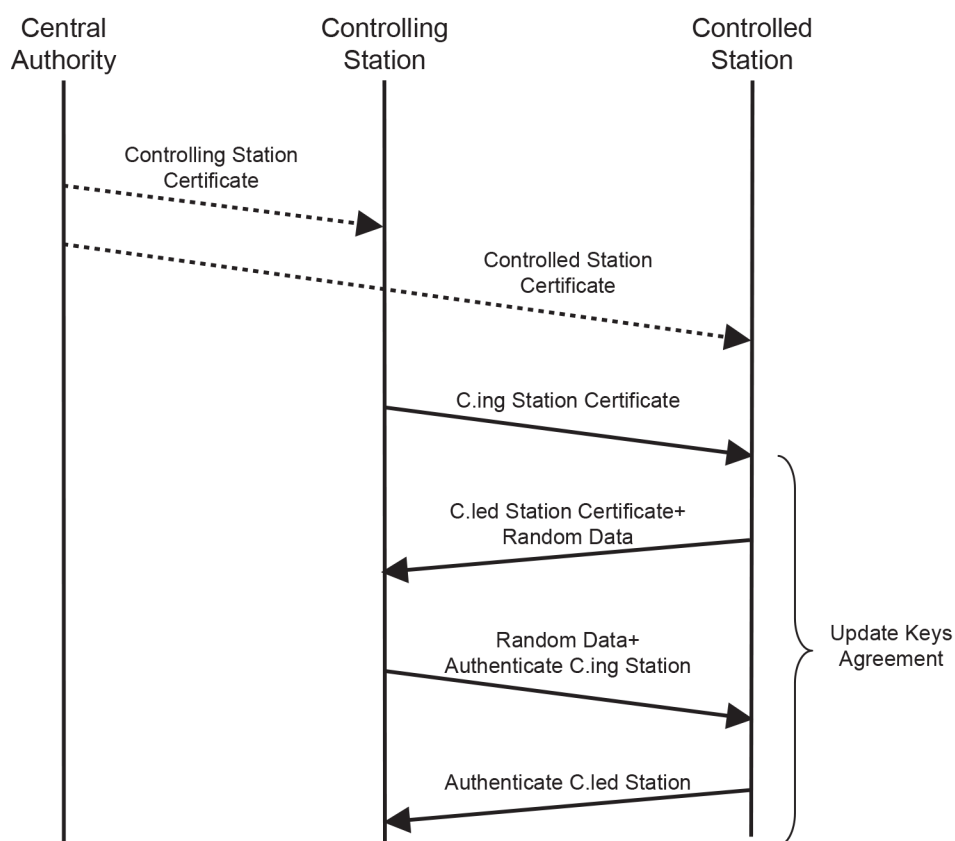


Figure 1 – Overview of interaction between Central Authority and Stations

IEC

6.2.7 Security statistics

An important feature of the secure communication mechanism is that it provides ability for the operators of the network to detect some kinds of attacks. Any controlled station implementing this secure communication 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 errors, 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 secure communication. This permits the operators of the network to detect attacks that may be occurring on other links than the one they are currently monitoring.

6.2.8 Security events

It is important that care be taken to log security-related violations in a separate log whose contents are inherently secure from manipulation (e.g., modification of information or deletion of information). Implementers should strive to archive enough information so that security audit and prosecution is facilitated. The actual implementation of this recommendation is a local matter.

Relevant communications and definitions pertaining to monitoring and security logging are addressed in two separate parts of IEC 62351: IEC 62351-7 addresses security monitoring in the context of network management, while IEC 62351-14 addresses security logging.

7 Functional requirements

7.1 Overview of clause

Clause 7 formally describes the functionalities required by this secure communication mechanism. If Clause 7 differs from Clause 6, Clause 7 shall be considered to take precedence.

The devices claiming conformance to this document shall implement the secure communication mechanism described in Clause 7 independently for each Association between a controlling station and a controlled station.

7.2 Procedures Overview

The secure communication mechanism defined in this document is composed of three procedures:

- a) Station Association
It is performed to create and update a controlling station/controlled station association with the controlling station role and the corresponding Update Keys.
- b) Session Key Change
It is executed after the Station Association and on regular basis renew the Session Keys by using the Update Keys.
- c) Secure Data Exchange
This is the operational state where the stations authenticate and exchange application data. The application data is secured by using the Session Keys.

Figure 2 shows the execution sequence of these procedures.

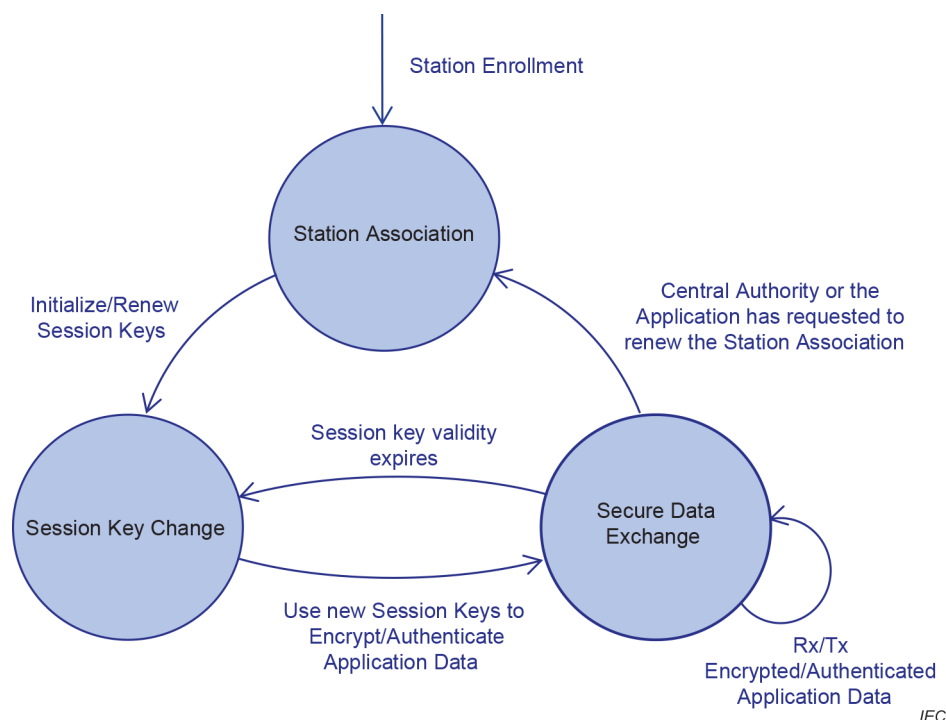


Figure 2 – Sequence of procedures

7.3 State machine overview

Table 4 and Table 5 describe the states used by the state machines in these procedures, in the general order in which they might be expected to occur.

As described in the state machine tables, some Station Association and Session Key Change states would be only momentary and the state machines would immediately return to the stable state after taking the appropriate action.

The controlling station should not execute the Station Association procedure and the Session Key Change procedure at the same time. For this reason, the Station Association and Session Key Change state machines share the “Key Management Idle” stable state.

The state machine shall be independent for each communication link with the remote stations (identified by the Association ID) in both controlling and controlled stations.

Table 4 – States used in the controlling station state machine

State	Procedure	Description
Key Management Idle	Station Association Session Key Change	This stable state is shared between the Station Association and the Session Key Change state machines. This is the state where the controlling station is not solicited to perform the Station Association procedure or the Session Key Change procedure. Update keys and Session Keys may be either valid or not valid.
Wait for Association Response	Station Association	The Station Association state machine enters in this transition state when the controlling station has transmitted an Association Request and is waiting for the Association Response from the controlled station.
Wait for Update Key Change Response.	Station Association	The Station Association state machine enters in this transition state when the controlling station has transmitted an Update Key Change Request and is waiting for the Update Key Change Response from the controlled station.
Wait for Session Response	Session Key Change	The Session Key Change state machine enters in this transition state when the controlling station has transmitted a Session Request and is waiting for the Session Response from the controlled station.
Wait for Session Key Change Response.	Session Key Change	The Session key Change state machine enters in this transition state when the controlling station has transmitted a Session Key Change Request and is waiting for the Session Key Change Response from the controlled station.
No Session	Secure Data Exchange	The Secure Data Exchange state machine enters in this stable state if the Session Keys are NOT valid. In this state the controlling station cannot exchange Secure Data messages with the controlled station.
Session Established	Secure Data Exchange	The Secure Data Exchange state machine enters in this stable state if the Session Keys are valid. In this state the controlling station exchanges Secure Data messages with the controlled station.
Secure Data Transmission Suspended.	Secure Data Exchange	The Secure Data Exchange state machine enters in this transition state when the Secure Data message transmission is suspended by the Session Key Change state machine. In this state, Secure Data message can be received but not transmitted.

Table 5 – States used in the controlled station state machine

State	Procedure	Description
Association Idle	Station Association	This is the stable state where the controlled station is not requested to execute the Station Association procedure by the controlling station. Update keys may be either valid or not valid.
Wait for Update Key Change Request.	Station Association	The Station Association state machine enters in this transition state when the controlled station has transmitted an Association Response and is waiting for the Update Key Change Request from the controlling station.
No Association	Session Key Change	The Session Key Change state machine enters in this stable state if the Update Keys are NOT valid. The Session Key Change cannot be executed.
Session Idle	Session Key Change	The Session Key Change state machine enters in this stable state if the Update Keys are valid. The Session Key Change can be executed.
Wait for Session Key Change Request.	Session Key Change	The Session key Change state machine enters in this transition state when controlled station has transmitted a Session Response and is waiting for the Session Key Change Request from the controlling station.
No Session	Secure Data Exchange	The Secure Data Exchange state machine enters in this stable state if the Session Keys are NOT valid. In this state the controlled station cannot exchange Secure Data messages with the controlling station.
Session Established	Secure Data Exchange	The Secure Data Exchange state machine enters in this stable state if the Session Keys are valid. In this state the controlled station exchanges Secure Data messages with the controlling station.

7.4 Timers and counters

This secure communication mechanism makes use of different timers and counters to control the execution of the procedures described in Clause 8. Table 6 summarizes these timers and counters, how they are used, the corresponding thresholds and the events correlated.

Table 6 – Summary of timers and counters used

Name	Use	Station Type	Threshold	Event in State Machine
Reply Timer	The controlling station uses this timer to verify that, upon a request sent, the corresponding response is received within the expected time.	Controlling	Expected Reply Time	Reply Timeout
Request Timer	The controlled station uses this timer to verify that a specific request is received within the expected time. In the controlled station, the Station Association and the Session Key Change state machines shall make use of two independent Request Timers.	Controlled	Expected Request Time	Request Timeout
Session Key Usage Timer	The station uses this timer to check the amount of time the Session Key has been used to authenticate Secure Data Messages since the last Session Key Change procedure successfully executed.	Controlling and controlled	Max Session Key Usage Time	Session Key Usage Time expired
Session Key Usage Counter	The station uses this counter to check the number of times the session key has been used to authenticate Secure Data Messages since the last Session Key Change procedure successfully executed. This counter is incremented by 1 each time a Secure Data Message is successfully processed.	Controlling and controlled	Max Session Key Usage Count	Session Key Usage Count exceeded

Each station shall permit the Timers/Counters thresholds listed in Table 6 to be configured. The measurement unit and configurable ranges of these thresholds are defined in the interoperability requirements of this document at subclause 9.2.6.

7.5 Security statistics and events

7.5.1 General

Stations shall monitor the use of this secure communication mechanism by counting a variety of protocol events using security statistic counters. For each event, the station shall permit security statistic counts of up to 4294967295 (32 bits). Table 7 summarizes the security statistics and describes the event counted.

The state machine tables in this secure communication mechanism describe the precise conditions under which the statistics are to be incremented, and the specific actions to be taken. The exception is the Total Messages Sent and Total Messages Received, which are incremented too frequently to be documented specifically.

Each security statistic counter has a specific security event associated. Each time a security statistic is incremented the corresponding security event should be announced as described in 7.5.3.

All the security statistic counters listed in Table 7 are mandatory to be implemented.

For each security statistic, Table 7 indicates the corresponding security event log mnemonic and NSM monitoring object as they are defined respectively in IEC 62351-14 and in IEC 62351-7. Annex A provides a mapping of the defined events in this document to the notion of IEC 62351-14.

If IEC 62351-14 is implemented the events described in Table 7 shall be applied. If IEC 62351-7 is implemented the monitoring object described in Table 7 shall be applied. The occurrence of each event is described in the corresponding state machine of each procedure.

Table 7 – Security statistics and associated events

Security Statistic Counter	Increment whenever...	Station type	Log event	Monitoring object
Successful Station Associations	The Station Association procedure has been successfully performed.	Controlling and controlled	STAS_PROC_SUCC <i>Notice: Station Association successfully performed</i>	StAsProcScsCnt <i>Number of times the Station Association procedure has been successfully performed</i>
Station Association Failures	The Station Association procedure has failed	Controlling and controlled	STAS_PROC_FAIL <i>Alarm: Station Association failed</i>	StAsProcFailCnt <i>Number of times the Station Association procedure has failed</i>
Successful Session Key Changes	The Session Key Change procedure has been successfully performed	Controlling and controlled	SKEY_PROC_SUCC <i>Notice: Session Key Change successfully performed</i>	SKeyProcScsCnt <i>Number of times the Session Key was changed successfully</i>
Session Key Change Failures	The Session Key Change procedure has failed	Controlling and controlled	SKEY_PROC_FAIL <i>Alarm: Session Key Change failed</i>	SKeyProcFailCnt <i>Number of Session Key Change failures</i>
Session Key Invalidations due Max Session Key Usage Time expired	During Secure Normal Operations, the Session Keys were invalidated because the controlling station did not change them within the Max Session Key Usage Time interval.	Controlled	SKEY_INV_USETOUT <i>Alarm: Session Key invalidated due to Max Session Key Usage Timeout</i>	SKeyInvToutCnt <i>Number of times the Session Keys were invalidated due to Max Session Key Usage Timeout</i>
Session Key Invalidations due Max Session Key Usage Count reached.	During Secure Normal Operations, the Session Keys were invalidated because the controlling station did not change them before reaching the Max Session Key Usage Count threshold.	Controlled	SKEY_INV_USECNT <i>Alarm: Session Key invalidated due to Max Session Key Usage Count</i>	SKeyInvUseCnt <i>Number of times the Session Key was invalidated due to Max Session Key Usage Count</i>
Protocol Information Errors	During the Station Association procedure, or the Session Key Change procedures, the Protocol Information value provided by controlling station is not permitted or not supported.	Controlled	PROT_INFO_ERR <i>Alarm: Invalid protocol information</i>	ProtInfoErrCnt <i>Number of protocol information errors</i>
Key Authentication Algorithm Support Failures	During the Station Association procedure, the selected key authentication algorithm is not permitted or not supported.	Controlled	KEY_AUTNALG_SUP <i>Alarm: Key authentication algorithm not supported</i>	KeyAutnAlgSupFailCnt <i>Number of key authentication algorithm support failures</i>
Key Wrap Algorithm Support Failures	During the Station Association procedure, the selected key wrap algorithm is not permitted or not supported.	Controlled	KEY_WRAPALG_SUP <i>Alarm: Key wrap algorithm not supported</i>	SKeyWrapAlgSupFailCnt <i>Number of key wrap algorithm support failures</i>

Security Statistic Counter	Increment whenever...	Station type	Log event	Monitoring object
Data Protection Algorithm Support Failures	During the Session Key Change procedure, the selected data protection algorithm is not permitted or not supported.	Controlled	DATA_PROTALG_SUP <i>Alarm: Data MAC/AEAD algorithm not supported</i>	DataProtAlgSupFailCnt <i>Number of Data authentication algorithm support failures</i>
Key Authentication Errors	During Station Association procedure or the Session Key Change procedure, the other station has provided invalid Key authentication information.	Controlling and controlled	KEY_AUTN_ERR <i>Alarm: Key authentication error</i>	SKeyAutnErrCnt <i>Number of Key authentication errors</i>
Data Authentication Errors	During Secure Data Exchange, the local station received a non-authentic Secure Data message.	Controlling and controlled	DATA_AUTN_ERR <i>Warning: Data authentication error</i>	DataAutnErrCnt <i>Number of non-authentic Secure Data messages received</i>
Unexpected Messages	The station receives a message that was not the expected in the current status of the state machine.	Controlling and controlled	UNXP_MSG_ERR <i>Warning: Unexpected message error</i>	UnxpMsgErrCnt <i>Number of unexpected messages received</i>
Max Reply Timeouts (See 7.5.2)	During the Station Association procedure or the Session Key Change procedure, the Max Reply Timeout threshold was reached.	Controlling	MAX_REPLY_TOUT <i>Warning: Max reply timeouts reached</i>	MaxReplyToutCnt <i>Number of times the Max Reply Timeouts threshold was reached</i>
Remote Station's Authorization Failures.	During the Station Association procedure, the local station receives a remote station's certificate from a station not authorized to communicate.	Controlling and controlled	NODE_NOT_AUTR <i>Alarm: Remote station not authorized</i>	NodeAutrFailCnt <i>Number of unauthorized communication attempts</i>
Operation Authorization Failures (See Note 2)	During Secure Data Exchange, the controlled station received an authentic Secure Data message but the controlling station is not authorized (has not the role/permission) to perform the requested operation.	Controlled	OPER_NOT_AUTR <i>Warning: Requested operation not authorized</i>	CtrlOperAutrFailCnt <i>Number of unauthorized operations</i>
Remote Station's Certificate Validity Check Failures.	During the Station Association procedure, the local station receives an expired or a revoked certificate or a certificate containing invalid parameters or invalid signature from the remote station	Controlling and controlled	REM_CERT_NOTVALID <i>Alarm: Invalid remote station's certificate</i>	RemCertCheckFailCnt <i>Number of invalid certificates received</i>
Remote Station's Certificate Expirations.	While the Station Association is established the remote station's certificate expired.	Controlling and controlled	REM_CERT_EXPIRED <i>Warning: Remote station's certificate expired.</i>	RemCertExpiredCnt <i>Number of times the remote station's certificate expired.</i>
Remote Station's Certificate Revocations. (See Note 1)	While the Station Association is established the remote station's certificate has been revoked by the Central Authority.	Controlling and controlled	REM_CERT_REVOKED <i>Alarm: Remote station's certificate revoked.</i>	RemCertRevokedCnt <i>Number of times the remote station's certificate has been revoked.</i>

Security Statistic Counter	Increment whenever...	Station type	Log event	Monitoring object
Local Station's Certificate Expirations.	While the Station Association is established the local station's certificate expired.	Controlling and controlled	LOC_CERT_EXPIRED <i>Warning: Local station's certificate expired.</i>	LocCertExpiredCnt <i>Number of times the local station's certificate expired.</i>
Local Station's Certificate Revocations. (See Note 1)	While the Station Association is established the local station's certificate has been revoked by the Central Authority.	Controlling and controlled	LOC_CERT_REVOKED <i>Alarm: Local station's certificate revoked.</i>	LocCertRevokedCnt <i>Number of times the local station's certificate has been revoked.</i>
Cryptographic Keys Invalidations due to Remote Station's Certificate Revocation. (See Note 1)	Cryptographic keys (Update Keys and Session Keys) were marked invalid because the remote station's certificate has been revoked by the Central Authority.	Controlling and controlled	KEYS_INV_REMCERTREV <i>Alarm: Cryptographic Keys invalidated due to remote station's certificate revocation.</i>	KeysInvRemCertRevCnt <i>Number of times the Cryptographic Keys were invalidated due to remote station's certificate revocation.</i>
Cryptographic Keys Invalidations due to Local Station's Certificate Revocation. (See Note 1)	Cryptographic keys (Update Keys and Session Keys) were marked invalid because the local station's certificate has been revoked by the Central Authority.	Controlling and controlled	KEYS_INV_LOCCERTREV <i>Alarm: Cryptographic Keys invalidated due to local station's certificate revocation.</i>	KeysInvLocCertRevCnt <i>Number of times the Cryptographic Keys were invalidated due to local station's certificate revocation.</i>
Successful Data Authentications	During Secure Normal Operations, the local station received an authentic Secure Data message.	Controlling and controlled	None.	DataAutnScsCnt <i>Number of authentic Secure Data messages received</i>
Reply Timeouts	During the Station Association procedure or the Session Key Change procedure, the controlled station has not replied within the Expected Reply Time.	Controlling	None.	ReplyToutCnt <i>Number of Reply Timeouts</i>
Request Timeouts	During the Station Association procedure or the Session Key Change procedure, the controlling station has not sent a request within the Expected Request Time.	Controlled	None.	RequestToutCnt <i>Number of Request Timeouts</i>
Total Messages Sent	The station sends an ASDU	Controlling and controlled	None.	TxPduCnt. <i>Number of transmitted PDUs</i>
Total Messages Received	The station receives an ASDU	Controlling and controlled	None.	RxPduCnt. <i>Number of received PDUs (including PDUs with errors)</i>
Discarded Messages	The station discards a received message.	Controlling and controlled	None.	DiscPduCnt <i>Number of discarded messages</i>

NOTE 1 This security statistic is applicable if the Central Authority is supported. See 8.3.9.

NOTE 2 This security statistic is applicable if the Central Authority and Role Base Access Control (RBAC) are supported. See 8.5.6.1.

7.5.2 Special security thresholds

In addition, the state machines shall use the following moving threshold to determine when to react to error conditions as specified in the formal procedures described in Clause 8:

- Max Reply Timeouts (controlling station only): Maximum number of reply timeouts allowed in a session expecting a specific response from the controlled station.

If this threshold is reached, the event shall cause the device to take specific actions – other than just reporting the event – as described in the state machine.

Each time the state machine "resets" the Max Reply Timeouts value, it shall add the configured threshold for that statistic to the current value of the Max Reply Timeouts. The controlling station shall reset the Max Reply Timeouts value of all associations at startup.

7.5.3 Security statistics reporting

Devices shall permit the security statistic to be accessed without modification or reported by using the affected protocol services or by other means.

Furthermore, the controlled station shall be able to report these security statistic counters to the controlling station by using methods appropriate to the affected protocol.

The method used to transmit security statistics by using the affected protocol must be defined in the affected protocol referencing standards.

Each station shall permit a threshold to be configured for each of the security statistics listed in Table 7. The controlled station shall transmit security statistic value to the controlling station each time the corresponding threshold value is reached.

Each time the controlled station transmits a statistic value, it shall "reset" the corresponding threshold to the current statistic value plus the value configured for that threshold. Devices shall reset all the threshold values at startup.

The default value of the security statistic thresholds must be defined in the affected protocol referencing standards.

7.5.4 Security events monitoring and logging

Events in this secure communication mechanism, described in Table 7, are defined as warnings and alarms. These security events are intended to support the error handling and thus to increase system resilience. Implementations should provide a mechanism for announcing security events.

Note that warnings and alarms are used to indicate the severity of an event from a security point of view. It is expected that an operator's security policy determines the final handling based on the operational environment.

It is recommended that the security events (notices, warnings and alarms) throughout the document are implemented by monitoring objects as specified by IEC 62351-7 and/or by log events as specified by IEC 62351-14. IEC 62351-7 defines the handling of security monitoring information, while IEC 62351-14 specifies the handling of security warning and security alarm messages.

Alternative methods for security monitoring and logging may be specified in the affected protocol referencing standards.

It is strongly recommended that the security warning and alarms throughout the document are logged locally on devices. The method to perform local logging, the number of logs and time the logs shall be retained is a local implementation issue and is outside the scope of this document.

8 Formal procedures

8.1 Overview of subclause

Clause 8 formally describes the security protocol procedures, messages and data exchanged in detail.

The devices claiming conformance to this standard shall implement the secure communication mechanism described in Clause 8 independently for each Association between a controlling station and a controlled station.

8.2 Distinction between messages and ASDUs

8.2.1 General

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 affected protocol referencing standards, 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.

8.2.2 Messages datatypes and notations

The datatypes used in this document, in the Messages Definition subclauses, are defined in IEC 60870-5-4.

8.3 Station Association procedure

8.3.1 General

The Station Association procedure is performed to establish an association between controlling station and controlled station, to identify the communication link between the two stations, the Role of the controlling station, and to generate the associated Update Keys. Each device shall maintain a unique set of Update Keys for each association established.

This procedure is performed during commissioning (installation of controlling station and/or controlled station) or when it is requested by the Central Authority each time a new certificate is provisioned to the controlling station or to the controlled station.

Depending on the organization's security policy, the Central Authority or authorized personnel may also require the controlling station to initiate the Station Association procedure, even on regular basis to renew the Update Keys periodically. The method to solicit the controlling station to initiate the Station Association procedure is outside the scope of this document.

Additional conditions to initiate the Station Association procedure may be specified in the affected protocol referencing standards.

This procedure implements the Elliptic Curve Diffie-Hellmann (ECDH) exchange using public key certificates and a Hash Key Derivation Function (HKDF) on the information exchanged to generate the Update Keys (according to RFC 5869 and RFC 7748).

8.3.2 Public key certificates

8.3.2.1 General

The Station Association procedure requires the use of public key certificates (device certificates). The device certificates shall be a X.509 certificate and the public key shall be an ECDH key. The minimum length of the device's public key shall be 256 bits.

The device certificates can be either self-signed by the device itself or signed by the Central Authority if the Central Authority is supported (optional).

The controlled station shall be able to uniquely identify each controlling station communicating to it, so this security mechanism requires that the *Distinguished Name (DN)* value in the device certificates shall be unique for each device in the organization.

Implementations claiming conformance to this document shall be able to support a public-key certificate of 8192 octets or fewer. The size of the public-key certificates depends on the organization's security policy.

Implementations claiming conformance to this document shall be able to support the exchanging of X.509 certificates in Distinguished Encoding Rule (DER) format. During the Station Association procedure, the X.509 certificates shall be transmitted in DER format.

8.3.2.2 Cryptographic curves

Table 8 lists the Elliptic Curves, mandatory and optional to be supported, used to generate the public/private key pair and to sign the X.509 certificates. Additional curves may be specified in the affected protocol referencing standards.

Table 8 – Elliptic curves

EC Curve	Specified in	Mandatory or optional to be supported (m/o)
Curve 25519	RFC 7748	m
Curve 448	RFC 7748	m
secp256k1	SEC2-V2	m
secp256r1	SEC2-V2	m
brainpoolP256r1	RFC 5639	o

RFC 7748 specifies all the parameters for generating each curve as well as the point of the curve used to generate the public and private keys.

Device's public/private Key pair in devices authorized to communicate shall be generated using the same curve, therefore the device's ECC certificates exchanged during the Station Association procedure must specify the same EC curve.

Note that the support of Curve 25519 and Curve 448 is only intended in the context of ECDH key agreement, not in the context of digital signatures.

For X.509 certificates digital signature, the EC curve used shall be either secp256k1 or secp256r1. Optionally brainpoolP256r1 may be supported.

8.3.2.3 Use of self-signed certificates

Devices claiming conformance to this standard shall support self-signed public key certificates.

If self-signed certificates are used, each device shall be pre-provisioned with the public key or the certificate fingerprint of the remote station's certificate that will be received during the Station Association procedure.

Device self-signed certificates shall be signed with the device's private key using the Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA-256 secure hash algorithm as defined in Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA) [X9.62].

The EC curve used in this secure communication mechanism to sign the self-signed certificates shall be Secp256k1 or Secp256r1 defined in SEC2-V2: Recommended Elliptic Curve Domain Parameters, Version 2.0. Optionally, the EC curve brainpoolP256r1 defined in RFC 5639 can be used if supported.

In this secure communication mechanism, self-signed certificates shall not contain RBAC information.

8.3.2.4 Use of certificates signed by the Central Authority.

If the Central Authority is supported, device certificates signed by the Central Authority can be used in the Station Association procedure. The Central Authority in this case becomes the issuing Certification Authority.

Certificates signed by the Central Authority can be signed either with ECDSA key or RSA key. If the Central Authority is supported, devices shall support certificates signed with both ECDSA or RSA keys. The hash algorithm used in the creation of the signature of ECDSA or RSA certificates shall be at least SHA-256.

For ECDSA signed certificates the minimum key length shall be 256 bits, for RSA signed certificates the minimum key length shall be 2048 bits.

If certificates signed with ECDSA key are used, the EC curve used in this secure communication mechanism to sign the public key certificates shall be Secp256k1 or Secp256r1 defined in SEC2-V2: Recommended Elliptic Curve Domain Parameters, Version 2.0. Optionally, the EC curve brainpoolP256r1 defined in RFC 5639 can be used if supported.

The use of public key certificates is only permitted in conjunction with the corresponding Central Authority's public key certificate. If the public key certificate of the Central Authority is not available at the local station, the remote station's public key certificate shall not be accepted by the local station.

In this secure communication mechanism certificates signed by the Central Authority may contain RBAC information. For support of RBAC in public key certificates, Profile A of IEC 62351-8 shall be supported.

8.3.2.5 Use of attribute certificates

If the Central Authority is supported, the controlling station can provide an attribute certificate (described in RFC 5755) to the controlled station in place of the public key certificate (e.g. to change RBAC information) if the corresponding device public key certificate was already provided to the controlled station in a previous successfully executed Station Association procedure or by other means.

The use of attribute certificate is only permitted in conjunction with the corresponding Central Authority's public key certificate. If the public key certificate of the Central Authority is not available at the controlled station, the attribute certificate shall not be accepted by the controlled station.

Also, the use of attribute certificate is only permitted in conjunction with the corresponding controlling station's public key certificate signed by the Central Authority. If the public key certificate of the controlling station is not available at the controlled station, the attribute certificate shall not be accepted by the controlled station.

Note that the usage of attribute certificates between the controlling station and controlled station can support use cases in which two legal entities access the substation component with different roles.

For support of RBAC using attribute certificates, Profile B of IEC 62351-8 shall be supported.

8.3.3 Configuration of authorized remote stations

Devices shall permit a user to configure a list of the public keys of the remote stations authorized to communicate with the local station. This requirement permits organization to use self-signed certificates if the central authority is not supported. This configuration shall be permitted only to authorized personnel. The method to identify and configure authorized remote stations on devices is out of scope of this standard. Note that the identification of a remote station should be done based on unique identifiers in the operator's domain.

8.3.4 Pre-requisites to initiate the Station Association procedure

Prior to initiate the Station Association procedure (e.g. during the device installation) each device shall be provisioned with the following items:

- a) The X.509 device certificate.
 - b) If devices generate (or are provisioned with) self-signed certificates:
 - The corresponding remote station's public key or certificate fingerprint shall be provisioned to devices.
- If devices are provisioned with certificates signed by the Central Authority:
- The controlling station shall be provisioned with the X.509 certificate of the Central Authority issuing the controlled station certificate.
 - The controlled station shall be provisioned with the X.509 certificate of the Central Authority issuing the controlling station certificate.

If the device is not provisioned with a valid X.509 certificate, the entire security mechanism described in this standard cannot be executed.

The provisioning of public key certificates and the remote station's public key on devices shall be permitted only to the Central Authority or authorized personnel. The method to provide the public key certificates and the remote station's public key on devices is out of scope of this standard.

If the provisioning of public key certificates to the devices is automated, it should follow one of the mechanisms described in IEC 62351-9.

8.3.5 Messages definition

8.3.5.1 General

Subclause 8.3.5 describes security messages and data exchanged in each security message executing the Station Association procedure. Figure 3 illustrates the messages and data exchanged in detail.

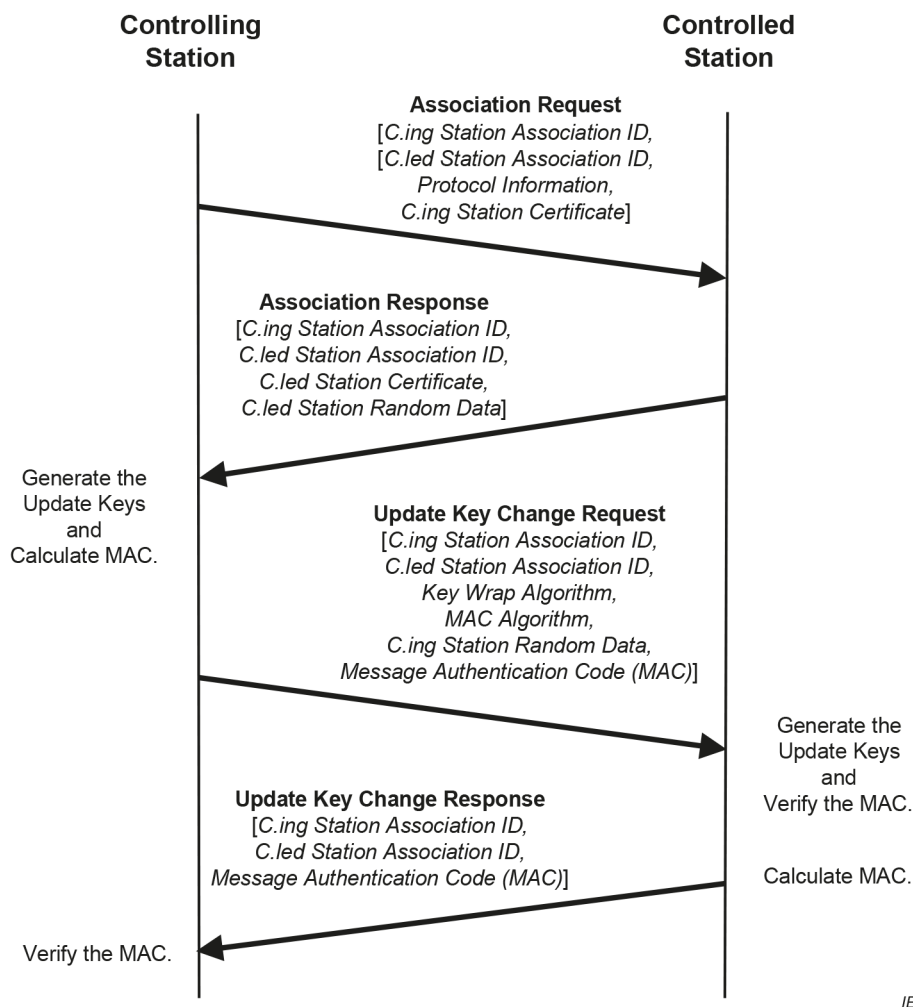


Figure 3 – Station Association procedure

8.3.5.2 Association Request message

8.3.5.2.1 Structure

Each Association Request message shall contain the information described in 8.3.5.2 and summarized in Table 9.

Only the controlling station shall send the Association Request message. The Association Request message shall elicit an Association Response message from the controlled station.

After sending the Association Request message, the controlling station shall start the Reply Timer to verify that the Association Response message is received from the controlled station within the expected time. If the Reply Timer expires (Reply Timeout), the controlling station shall execute the actions as indicated in the corresponding state machine described in 8.3.6.