IEC 62351-5

Edition 1.0 2023-01

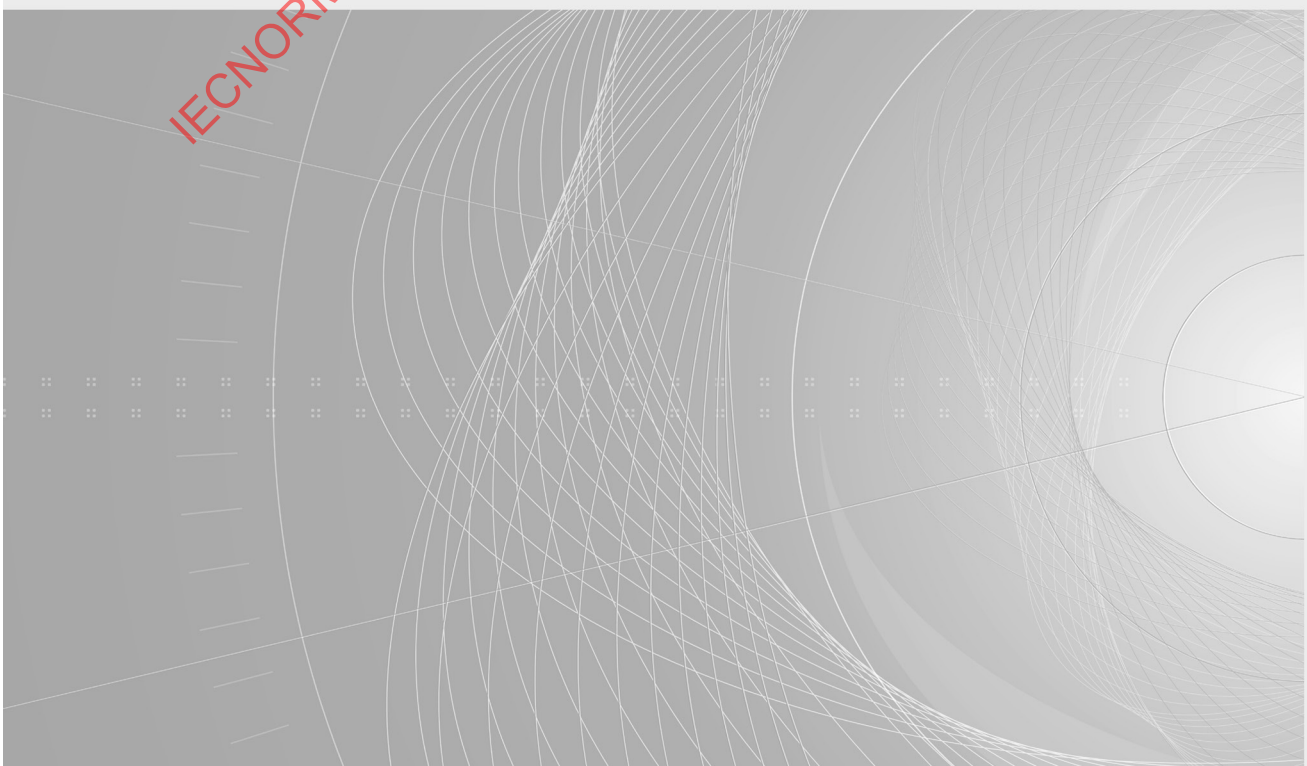
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés



IEC 62351-5:2023-01 (en-fr)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

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

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 62351-5

Edition 1.0 2023-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-6017-3

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 use 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

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

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.

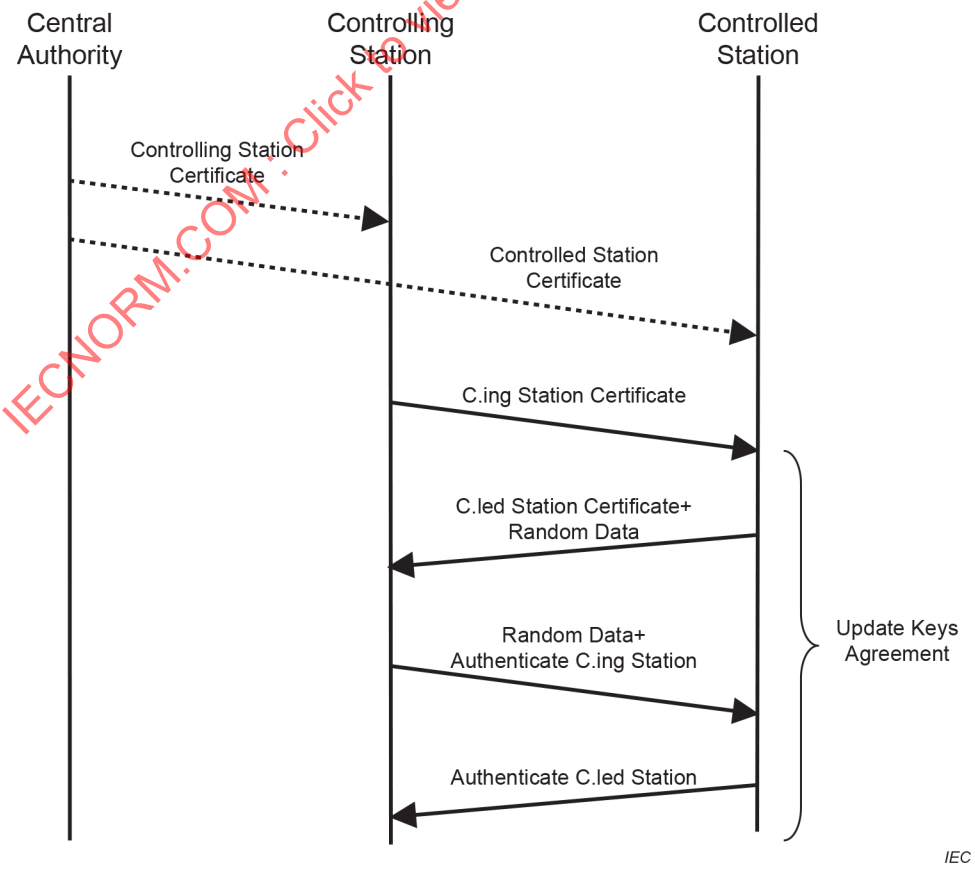


Figure 1 – Overview of interaction between Central Authority and stations

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.

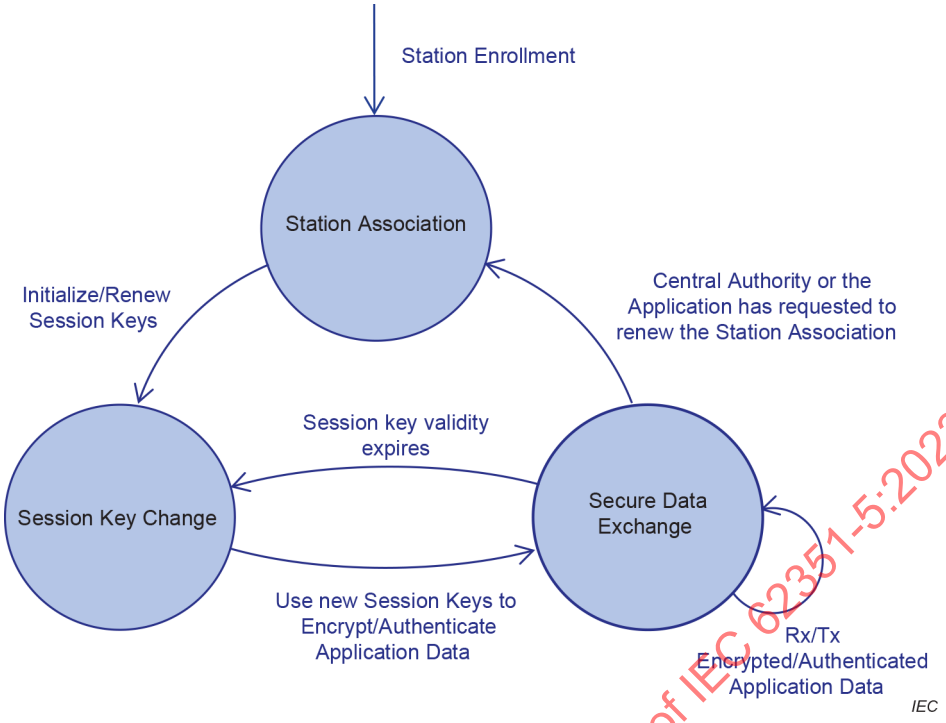


Figure 2 – Sequence of procedures

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 *Notice: Station Association successfully performed*	StAsProcScsCnt *Number of times the Station Association procedure has been successfully performed*
Station Association Failures	The Station Association procedure has failed	Controlling and controlled	STAS_PROC_FAIL *Alarm: Station Association failed*	StAsProcFailCnt *Number of times the Station Association procedure has failed*
Successful Session Key Changes	The Session Key Change procedure has been successfully performed	Controlling and controlled	SKEY_PROC_SUCC *Notice: Session Key Change successfully performed*	SKeyProcScsCnt *Number of times the Session Key was changed successfully*
Session Key Change Failures	The Session Key Change procedure has failed	Controlling and controlled	SKEY_PROC_FAIL *Alarm: Session Key Change failed*	SKeyProcFailCnt *Number of Session Key Change failures*
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 *Alarm: Session Key invalidated due to Max Session Key Usage Timeout*	SKeyInvToutCnt *Number of times the Session Keys were invalidated due to Max Session Key Usage Timeout*
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 *Alarm: Session Key invalidated due to Max Session Key Usage Count*	SKeyInvUseCnt *Number of times the Session Key was invalidated due to Max Session Key Usage Count*
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 *Alarm: Invalid protocol information*	ProtInfoErrCnt *Number of protocol information errors*
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 *Alarm: Key authentication algorithm not supported*	KeyAutnAlgSupFailCnt *Number of key authentication algorithm support failures*
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 *Alarm: Key wrap algorithm not supported*	SKeyWrapAlgSupFailCnt *Number of key wrap algorithm support failures*

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 *Alarm: Data MAC/AEAD algorithm not supported*	DataProtAlgSupFailCnt *Number of Data authentication algorithm support failures*
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 *Alarm: Key authentication error*	SKeyAutnErrCnt *Number of Key authentication errors*
Data Authentication Errors	During Secure Data Exchange, the local station received a non-authentic Secure Data message.	Controlling and controlled	DATA_AUTN_ERR *Warning: Data authentication error*	DataAutnErrCnt *Number of non-authentic Secure Data messages received*
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 *Warning: Unexpected message error*	UnxpMsgErrCnt *Number of unexpected messages received*
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 *Warning: Max reply timeouts reached*	MaxReplyToutCnt *Number of times the Max Reply Timeouts threshold was reached*
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 *Alarm: Remote station not authorized*	NodeAutrFailCnt *Number of unauthorized communication attempts*
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 *Warning: Requested operation not authorized*	CtrlOperAutrFailCnt *Number of unauthorized operations*
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 *Alarm: Invalid remote station's certificate*	RemCertCheckFailCnt *Number of invalid certificates received*
Remote Station's Certificate Expirations.	While the Station Association is established the remote station's certificate expired.	Controlling and controlled	REM_CERT_EXPIRED Warning: *Remote station's certificate expired.*	RemCertExpiredCnt *Number of times the remote station's certificate expired.*
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 Alarm: *Remote station's certificate revoked.*	RemCertRevokedCnt *Number of times the remote station's certificate has been revoked.*

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 Warning: *Local station's certificate expired.*	LocCertExpiredCnt *Number of times the local station's certificate expired.*
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 Alarm: *Local station's certificate revoked.*	LocCertRevokedCnt *Number of times the local station's certificate has been revoked.*
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 Alarm*: Cryptographic Keys invalidated due to remote station's certificate revocation.*	KeysInvRemCertRevCnt *Number of times the Cryptographic Keys were invalidated due to remote station's certificate revocation.*
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 Alarm*: Cryptographic Keys invalidated due to local station's certificate revocation.*	KeysInvLocCertRevCnt *Number of times the Cryptographic Keys were invalidated due to local station's certificate revocation.*
Successful Data Authentications	During Secure Normal Operations, the local station received an authentic Secure Data message.	Controlling and controlled	None.	DataAutnScsCnt *Number of authentic Secure Data messages received*
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 *Number of Reply Timeouts*
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 *Number of Request Timeouts*
Total Messages Sent	The station sends an ASDU	Controlling and controlled	None.	TxPduCnt. *Number of transmitted PDUs*
Total Messages Received	The station receives an ASDU	Controlling and controlled	None.	RxPduCnt. *Number of received PDUs (including PDUs with errors)*
Discarded Messages	The station discards a received message.	Controlling and controlled	None.	DiscPduCnt *Number of discarded messages*

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.

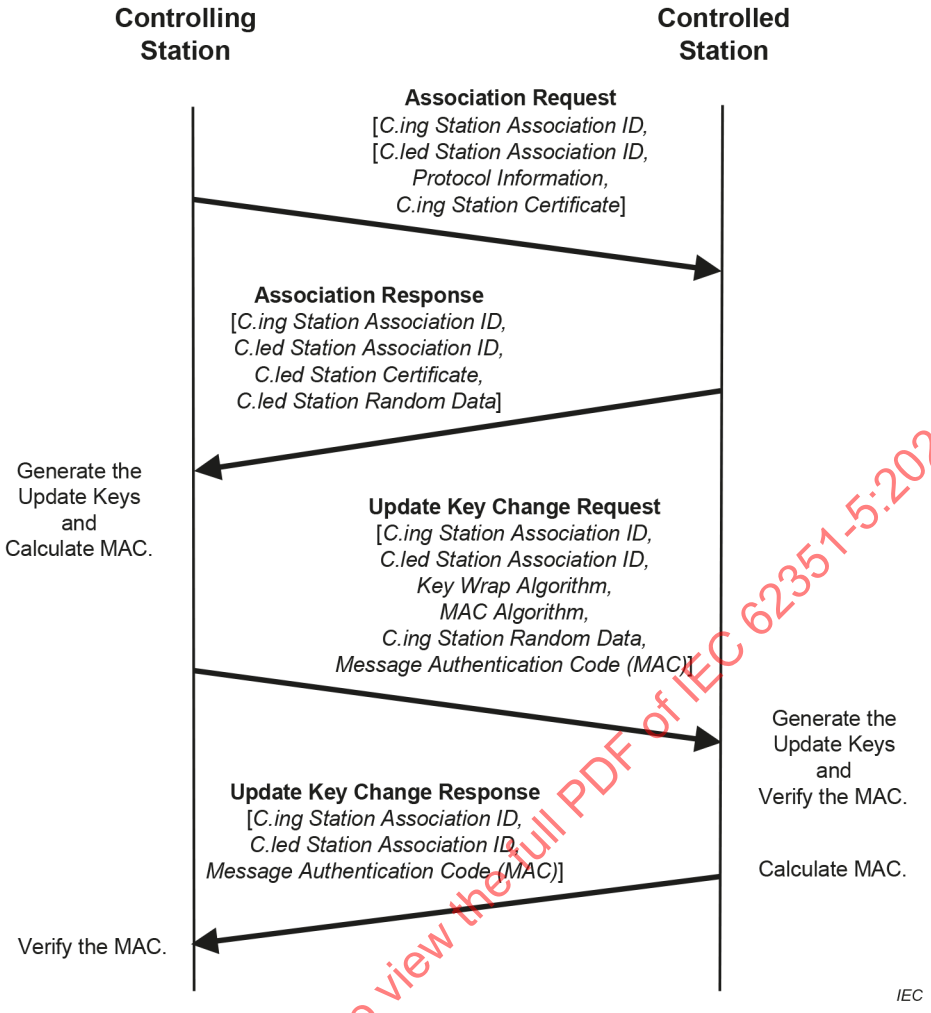


Figure 3 – Station Association procedure

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.

Table 9 – Association Request message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Value Value	PRI = Protocol Information
Value Value	CDL = Controlling station certificate data length
Number of octets specified in CDL	CDC = Controlling station certificate data

8.3.5.2.2 Controlling Station Association ID

This is the value the controlling station has chosen to represent the communication link with this controlled station. On the controlling station, this value shall be unique for each association with the controlled stations. Affected protocol referencing standards may require specific values of AIM in this message.

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

8.3.5.2.3 Controlled Station Association ID

This value is 0 (zero) per default in this message. Affected protocol referencing standards may require specific values of AIS in this message.

AIS:= UI16[1..16]<0>

8.3.5.2.4 Protocol Information

The controlling station uses this field to provide protocol information, including the protocol version, it intends to use to the controlled station.

The structure and the possible values in this field shall be specified by the affected protocol referencing standards.

Controlling and controlled stations may support multiple protocol versions. The controlled station shall validate the Protocol Information value specified in the Association Request message received. The rules to validate Protocol Information value on the controlled station shall be specified in the affected protocol referencing standards. If the Protocol Information value is considered not valid in the referencing standard, the controlled station shall ignore the Association Request received.

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

8.3.5.2.5 Controlling Station Certificate Data Length

The controlling station shall use this field to specify the length of the Controlling Station's X.509 Certificate data that follows.

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

8.3.5.2.6 Controlling Station Certificate Data

The controlling station shall use this field to provide the X.509 certificate to the controlled Station.

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

8.3.5.3 Association Response message

8.3.5.3.1 Structure

Each Association Response message shall contain the information described in 8.3.5.3 and summarized in Table 10.

The controlled station (only) shall send the Association Response message each time a valid Association Request message is received from the controlling station.

The Association Response message provides the controlled station's certificate and the associated random data to the controlling station, the controlling station must use this information to authenticate the subsequent Update Key Change Request message.

After sending the Association Response message, the controlled station shall start the Request Timer to verify that the subsequent Update Key Change Request message is received from the controlling station within the expected time. If the Request Timer expires (Request Timeout), the controlled station shall execute the actions as indicated in the corresponding state machine described in 8.3.7.

The Request Timer shall be stopped when a valid Update Key Change Request message is received.

Table 10 – Association Response message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Value Value	CDL = Controlled station certificate data length
Value	CGL = Controlled station random data length
Number of octets specified in CDL	CDC = Controlled station certificate data
Number of octets specified in CGL	CGD = Controlled station random data

8.3.5.3.2 Controlling Station Association ID

This value shall match the AIM in the Association Request message most recently received from the controlling station, described in 8.3.5.2.

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

8.3.5.3.3 Controlled Station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. On the controlled station, this value shall be unique for each association established with the controlling stations. Affected protocol referencing standards may require specific values of AIS in this message.

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

8.3.5.3.4 Controlled Station Certificate Data Length

The controlled station shall use this field to specify the length of the controlled station's X.509 device certificate data that follows.

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

8.3.5.3.5 Controlled Station Random Data Length

This value shall specify the length in octets of the random data that follows. The minimum length of the random data in this message shall be four octets, the maximum length is 64 octets.

CGL:= UI8[1..8]<4 ..64>

8.3.5.3.6 Controlled Station Certificate Data

The controlled station shall use this field provide the X.509 certificate to the controlling station.

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

8.3.5.3.7 Controlled Station Random Data

The controlled station shall include this random data in the Association Response message to ensure that the contents of the subsequent Update Key Change Request message are not predictable. This random data is also used to derive the Update Keys as described in 8.3.10.

Random number generators are responsible for providing statistically adequate random data. Guidance for random number generation can be found in NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C as well as in IETF RFC 4086.

CGD:= OS8i[1..8i]; i:=CGL

8.3.5.4 Update Key Change Request message

8.3.5.4.1 Structure

Each Update Key Change Request message shall contain the information described in 8.3.5.4 and summarized in Table 11.

Only the controlling station shall send Update Key Change Request messages. The Update Key Change Request message provides information used by the controlled Station to calculate and verify the Update Keys.

After sending the Update Key Change Request message, the controlling station shall start the Reply Timer to verify that the Update Key Change 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 state machine described in 8.3.6.

Table 11 – Update Key Change Request message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Enumerated value	KWA = Session Key wrap algorithm
Enumerated value	MAL = MAC algorithm
Value	CGL = Controlling station random data length
Number of octets specified in CCL	CGD = Controlling station random data
Number of octets specified by the MAC algorithm (MAL) selected in this message, defined in 8.3.5.4.5	MAC = Message authentication code

8.3.5.4.2 Controlling Station Association ID

This is the value the controlling station has chosen to represent the communication link with this controlled station. On the controlling station, this value shall be unique for each association with the controlled stations. This value cannot be 0 (zero).

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

8.3.5.4.3 Controlled Station Association ID

This value shall match the AIS in the Association Response message most recently received from the controlled station, described in 8.3.5.3.

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

8.3.5.4.4 Session Key Wrap Algorithm

Using this field, the controlling station shall indicate to the controlled station the selected algorithm used to encrypt/decrypt the Session Keys during the Session Key Change procedure, described in 8.4.

The key wrap algorithms mandatory to be supported are listed in Clause 9: Interoperability requirements. The best available option should be selected in this field.

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

<0>:= not used

<1>:= obsoleted

<2>:= AES-256 Key Wrap Algorithm

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

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

8.3.5.4.5 MAC Algorithm

Using this field, the controlling station shall indicate to the controlled station the selected algorithm to calculate MAC values and its resulting length in the authenticated messages exchanged in this authentication session (Update Key Change Request, Update Key Change Response) as well as in the authenticated messages exchanged in all subsequent Session Key Change procedures performed (Session Key Change Request, Session Key Change Response) described in 8.4.

The MAC algorithms mandatory to be supported are listed in Clause 9: Interoperability Requirements. The best available option should be selected in this field.

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

<0>:= reserved

<1>:= reserved

<2>:= obsoleted

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

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

<5>:= obsoleted

<6>:= obsoleted

<7>:= HMAC-SHA3-256 truncated to 8 octets (serial)

<8>:= HMAC-SHA3-256 truncated to 16 octets (networked)

<9>:= BLAKE2s-256 truncated to 8 octets (serial)

<10>:= BLAKE2s-256 truncated to 16 octets (networked)

<11..127>:= reserved for future use

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

8.3.5.4.6 Controlling Station Random Data Length

The controlling station shall use this field to specify the length of the random data that follows. The minimum length of the random data shall be four octets, the maximum length is 64 octets.

CGL:= UI8[1..8]<4 ..64>

8.3.5.4.7 Controlling Station Random Data

The controlling station shall send this data to avoid replay attacks on the changing of Update Keys. This random data is also used to derive the Update Keys as described in 8.3.10. Random number generators are responsible for providing statistically adequate random data. Guidance for random number generation can be found in NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C as well as in IETF RFC 4086.

CGD:= OS8i[1..8i]; i:=CGL

8.3.5.4.8 Message Authentication Code

The controlling station shall use this field to authenticate the data included in Update Key Change Request message being transmitted.

This value shall be calculated using the MAC algorithm selected in this message, described in 8.3.5.4.5, using the corresponding **Authentication Update Key** generated as described in 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 12, the referencing standards may require further information, in addition to those indicated in Table 12 to be included in the MAC calculation. The length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.3.5.4.5.

Table 12 – Data Included in MAC calculation (in order)

Data	Description	Described in	Source
Controlled Station Random Data	The random data provided by the controlled station in the Association Response message most recently received.	Subclause 8.3.5.3.7	Association Response
Update Key Change Request values	The entire Update Key Change Request message being transmitted up to and including CGD (excluding the MAC field).	Subclause 8.3.5.4	Update Key Change Request
Padding data	Additional padding data required by the MAC algorithm.	Algorithm specification.	Required by algorithm.

MAC:= OS8i[1..8i]; i:=as specified in MAL of this message, defined in 8.3.5.4.5.

8.3.5.5 Update Key Change Response message

8.3.5.5.1 Structure

Each Update Key Change Response message shall contain the information described in 8.3.5.5 and summarized in Table 13.

Only the controlled station shall send Update Key Change Response message. Exchanging this message ensures that both controlling station and controlled station agree on the following information:

– the identity of both the controlling station and the controlled station,
– the new Update Keys,
– the controlling Station Association ID (AIM) that the controlling station will associate to these Update Keys in all subsequent authentications.
– the controlled Station Association ID (AIS) that the controlled station will associate to these Update Keys in all subsequent authentications.
– The Role of the controlling station on this controlled station (if Central Authority and RBAC are supported).

Table 13 – Update Key Change Response message

Value	AIM = Controlling station association ID
Value	
Value	AIS = Controlled station association ID
Value	
Number of octets specified by the MAC algorithm (MAL) selected in the valid Update Key Change Request most recently received, defined in 8.3.5.4.5	MAC = Message authentication code

8.3.5.5.2 Controlling Station Association ID

This value shall match the AIM in the Update Key Change Request message most recently received from the controlling station, described in 8.3.5.4.2.

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

8.3.5.5.3 Controlled Station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. On the controlled station, this value shall be unique for each association established with the controlling stations. This value cannot be 0 (zero).

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

8.3.5.5.4 Message Authentication Code

The controlling station shall use this field to authenticate the data included in Update Key Change Response message being transmitted.

This value shall be calculated using the MAC algorithm selected in the Update Key Change Request most recently received, described in 8.3.5.4.5, using the corresponding Authentication Update Key generated as described in 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 14, the length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.3.5.4.5.

Table 14 – Data Included in MAC calculation (in order)

Data	Description	Described in	Source
Update Key Change Request values	The entire Update Key Change Request message most recently received	Subclause 8.3.5.4	Update Key Change Request
Update Key Change Response values	The entire Update Key Change Response message being transmitted up to and including AIS (excluding the MAC field).	Subclause 8.3.5.5	Update Key Change Response
Padding data	Additional padding data required by the MAC algorithm.	Algorithm specification.	As required by algorithm.

MAC:= OS8[1..8i]; i:=as specified in MAL of the Update Key Change Request message most recently received, defined in 8.3.6.4.5.

8.3.5.6 Association procedure solicited by the controlled station

If spontaneous unsolicited messages from the controlled station are permitted, the controlled station may optionally solicit the controlling station to initiate the Association procedure by sending an Association Initiation Request message. The affected protocol referencing standards may define the Association Initiation Request message and its management.

8.3.5.7 Supporting of concurrent associations on controlled station

It is strongly recommended for the controlled station to limit the number of concurrent associations supported. The controlled station is permitted to not respond to any Association Request if this limit is exceeded.

8.3.6 Controlling station state machine

On controlling station, the Station Association messages described in 8.3.5 shall be managed by the state machine described in 8.3.6. Figure 4 illustrates an overview of the Station Association transactions on controlling station. The controlling station shall execute the Station Association state machine described in Table 15. The *Key Management Idle* state is shared (in common) with the Session Key Change state machine.

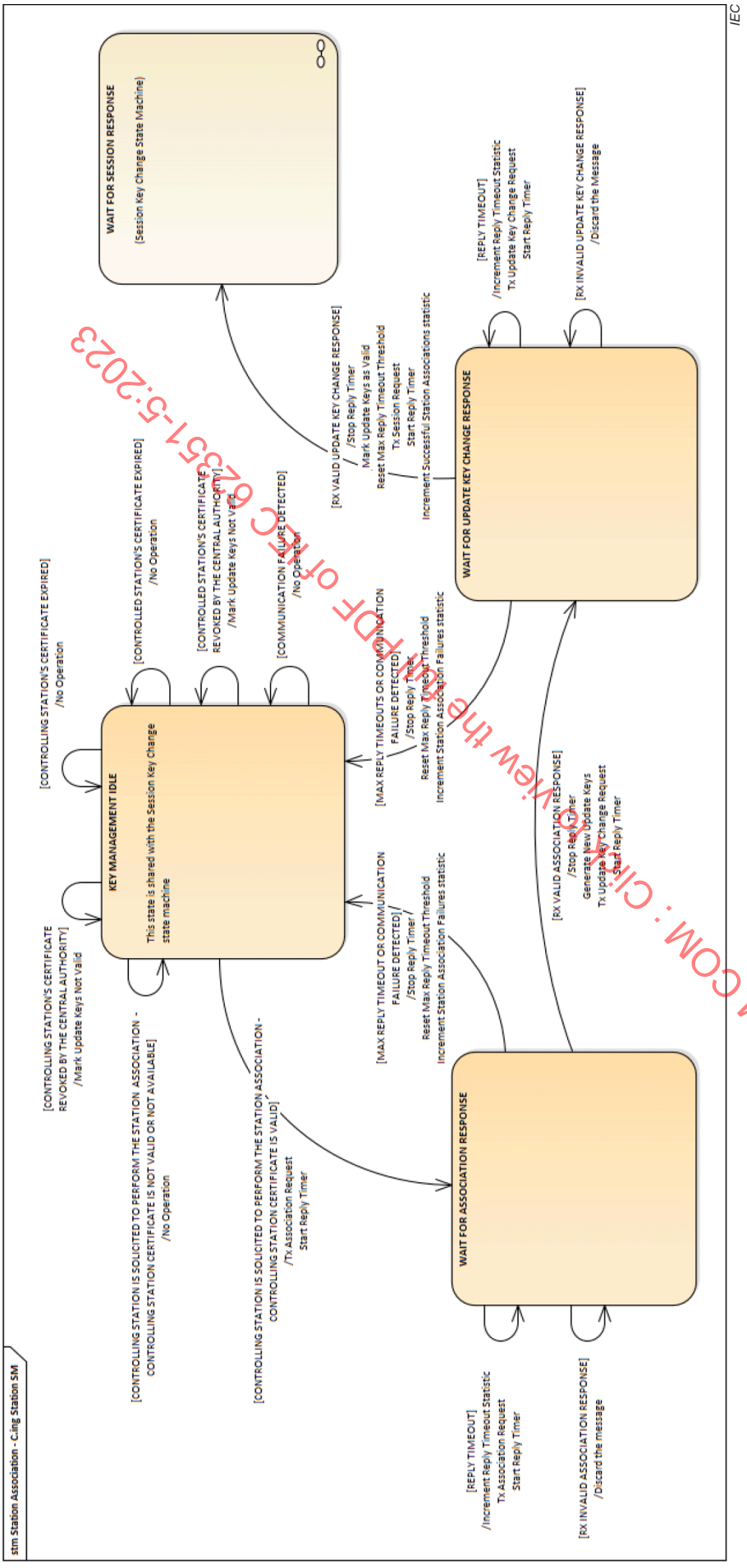


Figure 4 – Station Association – Controlling station state machine

Table 15 – Controlling station state machine: Station Association

Event	Event Description	State						
		Key Management Idle (this state is shared with the Session Key Change state machine)		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Controlling station is solicited to perform the Station Association	The Central Authority or the Application has requested to perform the Station Association procedure.	IF the controlled station's certificate is Valid: – Transmit the Session Request message. – Start the Reply Timer	Wait for Association Response	Discard the event. (The controlling station is already executing the procedure in this state)	Wait for Association Response	Discard the event. (The controlling station is already executing the procedure in this state)	Wait for Update Key Change Response	1
		IF the controlled station's certificate is Not Valid or Not Available: – No Operation	Key Management Idle					
Rx Valid Association Response	The controlling station has received an Association Response message with valid parameters and a valid controlled station's certificate.	Increment *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Stop Reply Timer Generate the new Update Key Transmit the Update Key Change Request message. Start the Reply Timer.	Wait for Update Key Change Response	Increment *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	2

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Session Key Change state machine)**		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Association Response: the message contains parameter error(s).	The controlling station has received an Association Response with one of the following error conditions: a) The controlling station Association ID does not match that in the Association Request b) The Random Data Length is less than minimum required c) The Random Data Length is over the maximum allowed.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	3

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Session Key Change state machine)**		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Association Response: the controlled station's certificate is NOT valid.	The controlling station has received an Association Response with one of the following error conditions: a) The controlled station's certificate is expired. b) The controlled station's certificate is revoked by the Central Authority. c) The controlled station's certificate signature is not valid. d) The length of the public key is less that the minimum required. e) The EC Curve specified is not permitted or not supported or it does not match the EC curve specified in this controlling station's certificate.	Increment *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Remote Station's Certificate Validity Check Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Increment *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	4

Event	Event Description	State						
		Key Management Idle (this state is shared with the Session Key Change state machine)		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Association Response: the controlled station is not authorized to communicate.	The controlling station received an Association Response with one of the following error conditions: a) The controlled station's certificate is signed by the CA and this controlling station is not provisioned with the corresponding CA certificate. b) The controlled station's certificate is self-signed and this controlling station is not provisioned with the corresponding public key. c) The controlled station's certificate is signed by the CA and no AoR string in the controlled station's certificate correspond to the AoR strings assigned to this controlling station. d) The controlled station's certificate identifies a station not authorized to communicate with this controlling station by configuration.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Remote Station Authorization Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	5

Event	Event Description	State						
		Key Management Idle (this state is shared with the Session Key Change state machine)		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Valid Update Key Change Response	The controlling station received a correctly authenticated Update Key Change Response with valid parameters.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Stop Reply Timer Mark the Update key as Valid. Increment the *Successful Station Association* statistic. Reset Max Reply Timeouts threshold Transmit the Session Request message. Start Reply Timer	Wait for Session Response (Session Key Change procedure)	6
Rx Invalid Update Key Change Response: the message is not authentic.	The controlling station received an Update Key Change Response message with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Increment the *Key Authentication Errors* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	7

Event	Event Description	State						
		Key Management Idle (this state is shared with the Session Key Change state machine)		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Update Key Change Response: the message contains parameter error(s)	The controlling station received a correctly authenticated Update Key Change Response message with one of the following error conditions: a) The controlling station Association ID is incorrect. b) The controlled station Association ID is incorrect.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Association Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Response	**8**
Reply Timeout	The Reply Timer has expired while the controlling station was waiting for a response from the controlled station and the Reply Timeouts statistic has not reached the Max Reply Timeouts threshold	Discard the event. (This event can occur only when the state machine is in the "*Wait for Association Response*" state or in the "*Wait for Update Key Change Response*" state)	Key Management Idle	Increment the *Reply Timeouts* statistic. Transmit the Association Request message Start the Reply Timer.	Wait for Association Response	Increment the *Reply Timeouts* statistic. Re-transmit the last Update Key Change Request message transmitted Start the Reply Timer.	Wait for Update Key Change Response	**9**
Max Reply Timeouts	The current station association procedure has failed because the Reply Timeout statistic has reached Max Reply Timeouts threshold while the controlling station was waiting for a response from the controlled station.	Discard the event. (This event can occur only when the state machine is in the "*Wait for Session Response*" state or in the "*Wait for Session Key Change Response*" state)	Key Management Idle	Increment the Max *Reply Timeouts* statistic. Reset Max Reply Timeouts threshold. Increment the *Station Association Failures* statistic	Key Management Idle	Increment the Max *Reply Timeouts* statistic. Reset Max Reply Timeouts threshold. Increment the *Station Association Failures* statistic	Key Management Idle	**10**

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Session Key Change state machine)**		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Communication Failure Detected Note: this event shall be considered if communication failures can be detected in the communication link.	The station has detected a communication failure.	No Operation.	Key Management Idle	Stop Reply Timer. Reset Max Reply Timeouts threshold Increment the *Station Association Failures* statistic.	Key Management Idle	Stop Reply Timer. Reset Max Reply Timeouts threshold Increment the *Station Association Failures* statistic.	Key Management Idle	**11**
The controlling station's certificate has been revoked.	While the Station Association is established the controlling station's certificate has been revoked by the Central Authority.	Mark Update Keys as Not Valid Increment the *Local Station's Certificate Revocations* statistic. Increment the *Cryptographic Keys Invalidations due to Local Station's Certificate Revocation* statistic.	Key Management Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Association Response	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Response	**12**
The controlling station's certificate expired.	While the Station Association is established the controlling station's certificate validity expired.	No further operation is required other than Increment the Local Station's Certificate Expirations statistic.	Key Management Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Association Response	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Response	**13**

Event	Event Description	State						
		Key Management Idle (this state is shared with the Session Key Change state machine)		**Wait for Association Response**		**Wait for Update Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Association Request		The controlling station is waiting for the controlled station to send the response to the Update Key Change Request.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
The controlled station's certificate has been revoked.	While the Station Association is established the controlled station's certificate has been revoked by the Central Authority.	Mark Update Keys as Not Valid Increment the *Remote Station's Certificate Revocations* statistic. Increment the *Cryptographic Keys Invalidations due to Remote Station's Certificate Revocation* statistic.	Key Management Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Association Response	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Response	**14**
The controlled station's certificate expired.	While the Station Association is established the controlled station's certificate validity expired.	No further operation is required other than Increment the Remote Station's Certificate Expirations statistic.	Key Management Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Association Response	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Response	**15**

8.3.7 Controlled station state machine

On controlled station, the Station Association procedure messages described in 8.3.5 shall be managed by the state machine described in 8.3.7. Figure 5 illustrates an overview of the Station Association transactions on controlled station. The controlled station shall execute the Station Association state machine described in Table 16.

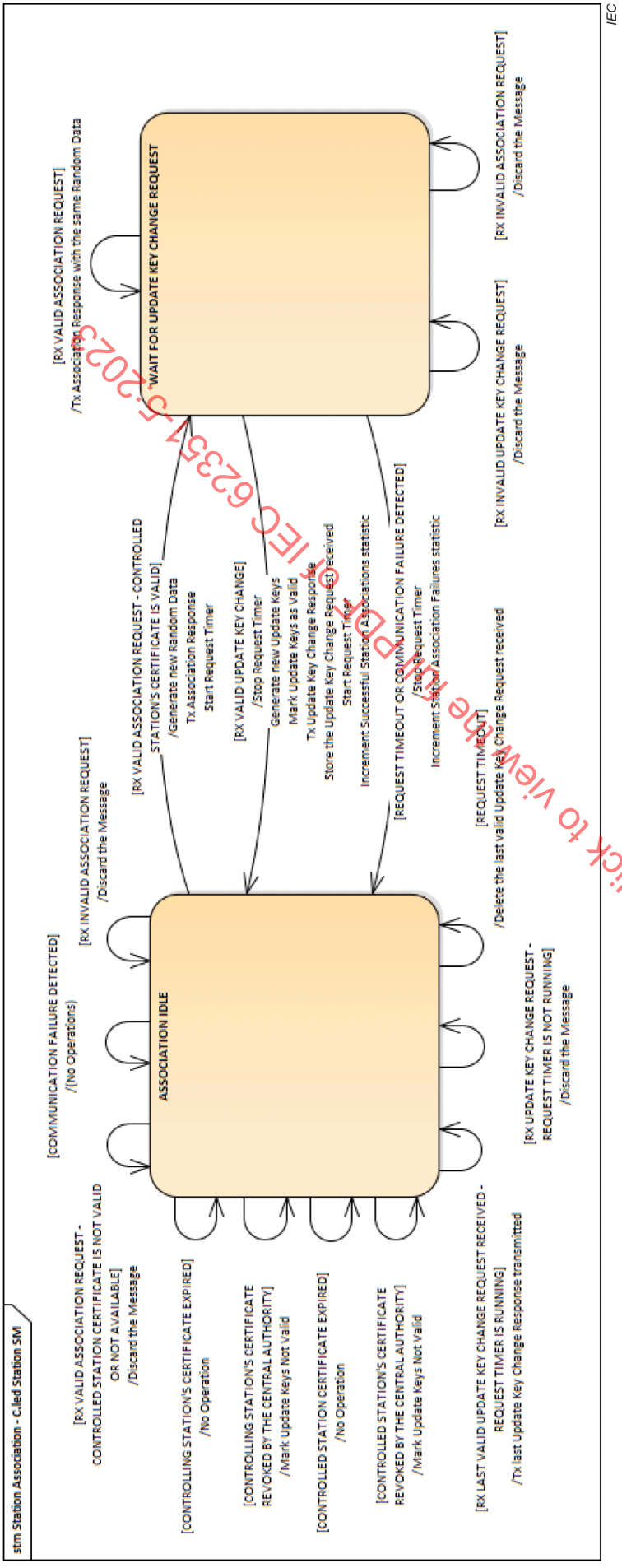


Figure 5 – Station Association – Controlled station state machine

Table 16 – Controlled station state machine: Station Association

Event	Event Description	State				
		Association Idle		**Wait for Update Key Change Request**		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	
Rx Valid Association Request	The controlled station has received a valid Association	IF the controlled station's certificate is Valid: – Generate new random data to be transmitted. – Transmit the Association Response with the new random data generated. – Start Request Timer	Wait for Update Key Change Request	Transmit the Association Response with the same random data provided in the last Association Response transmitted	Wait for Update Key Change Request	**1**
		IF the controlled station's certificate is Not Valid or Not Available: – Discard the message – Increment the *Discarded Messages* statistic	Association Idle			**2**
Rx Invalid Association Request: Protocol Information Error.	The controlled station receives an Association Request specifying a Protocol Information value not permitted or not supported	Increment the *Protocol Information Errors* statistic Discard the message Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Protocol Information Errors* statistic Discard the message Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	**3**

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Invalid Association Request: the controlling station's certificate is NOT Valid.	The controlled station has received an Association Request with one of the following error conditions: a) The controlling station's certificate is expired. b) The controlling station's certificate is revoked by the Central Authority. c) The controlling station's certificate signature is not valid. d) The length of the public key is less that the minimum required. e) The EC Curve specified is not permitted or not supported or it does not match the EC curve specified in this controlling station's certificate.	Increment the *Remote Station's Certificate Validity Check Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Remote Station's Certificate Validity Check Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	4

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Invalid Association Request: The controlling station is not authorized to communicate.	The controlled station has received an Association Request with one of the following error conditions: a) The controlling station's certificate is signed by the CA and this controlled station is not provisioned with the corresponding CA certificate. b) The controlling station's certificate is self-signed and this controlled station is not provisioned with the corresponding public key. c) The controlled station's certificate is signed by the CA and no AoR string in the controlling station's certificate correspond to the AoR strings assigned to this controlled station d) The controlling station's certificate identifies a station not authorized to communicate with this controlling station by configuration	Increment the *Remote Station Authorization Failures* statistic Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Remote Station Authorization Failures* statistic Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	5

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Valid Update Key Change Request	The controlled station received a correctly authenticated Update Key Change Request with valid parameters.	IF Request Timer is running AND the Update Key Change Request is identical to last valid Update Key Change Request received: – Retransmit the Update Key Change Response most recently transmitted ELSE: – Increment the *Unexpected Messages* statistic. – Discard the message. – Increment the *Discarded Messages* statistic	Association Idle	Stop Request Timer. Generate new Update Keys Mark the Update Keys as Valid Transmit the Update Key Change Response. Store the Update Key Change Request received Start Request Timer Increment the *Successful Station Associations* statistic.	Association Idle	6
Rx Invalid Update Key Change Request: the message is NOT authentic.	The controlled station received an Update Key Change Request message with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Key Authentication Errors* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	7

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Invalid Update Key Change Request: the message contains parameter error(s).	The controlled station receives a correctly authenticated Update Key Change Request but with one of the following error conditions: a) The controlled station Association ID does not match that in the last Association Response transmitted b) The Random Data Length is less than minimum required c) The Random Data Length is over the maximum allowed.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	8
Rx Invalid Update Key Change Request: Key authentication algorithm not permitted.	The controlled station receives an Update Key Change Request specifying a key authentication algorithm (MAL) that is not permitted or not supported.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Key Authentication Algorithm Support Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	9

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
Rx Invalid Update Key Change Request: Key wrap algorithm not permitted.	The controlled station receives a correctly authenticated Update Key Change Request specifying a key wrap algorithm (KWA) that is not permitted or not supported.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Association Idle	Increment the *Key Wrap Algorithm Support Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Update Key Change Request	10
Request Timeout	The Request Timer has expired while the controlled station was waiting for a valid Update Key Change Request from the controlling station.	Delete the last valid Update Key Change Request received.	Association Idle	Increment the *Request Timeouts* statistic. Increment the *Station Association Failures* statistic.	Association Idle	11
Communication Failure Detected Note; this event shall be considered if communication failures can be detected in the communication link	The controlled station has detected a communication failure	No Operations.	Association Idle	Stop Request Timer. Increment the *Station Association Failures* statistic.	No Association	12
The controlling station's certificate has been revoked.	The controlling station's certificate has been revoked by the Central Authority.	Mark Update Keys as Not Valid Increment the *Remote Station's Certificate Revocations* statistic. Increment the *Cryptographic Keys Invalidations due to Remote Station's Certificate Revocation* statistic	Association Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Request	13

Event	Event Description	State				
		Association Idle		Wait for Update Key Change Request		
		Stable state to manage Station Association and Update Keys The controlled station did not receive a valid Association Request from the controlling station		The controlled station is waiting for an Update Key Change Request from the controlling station		
		Action	Next State	Action	Next State	
A	B	C	D	E	F	
The controlling station's certificate expired.	The controlling station's certificate validity expired.	No further operation is required other than Increment the *Remote Station's Certificate Expirations* statistic.	Association Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Request	**14**
The controlled station's certificate has been revoked.	The controlling station's certificate has been revoked by the Central Authority.	Mark Update Keys as Not Valid Increment the *Local Station's Certificate Revocations* statistic Increment the *Cryptographic Keys Invalidations due to Local Station's Certificate Revocation* statistic	Association Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Request	**15**
The controlled station's certificate expired.	The controlling station's certificate validity expired.	No further operation is required other than Increment the *Local Station's Certificate Expirations* statistic.	Association Idle	This condition shall not be checked in this state since the new Station Association is not yet established.	Wait for Update Key Change Request	**16**

8.3.8 Verification of remote station's certificate

8.3.8.1 General

During the Station Association procedure, both controlling and controlled stations shall verify the validity of the certificate provided by the remote station by performing the operation described below, additional verifications may be required by the affected protocol referencing standards (also refer to IEC 62351-9 Ed.2 for the verification of CA provided certificates).

If one of the certificate verifications fails the local station shall consider the remote station's certificate not valid and shall interrupt the Station Association Procedure (the controlling station shall not send the subsequent the Update Key Change Request message, the controlled station shall not respond with the Association Response message).

If the current Update Keys are valid, the local station shall not invalidate the Update Keys if the remote station's certificate verifications fail.

If the Station Association is successfully performed, the certificate data received from the remote station shall be stored permanently on the local station, so that this procedure shall not be executed after a station initialization or after a communication failure.

8.3.8.2 Verification of self-signed certificate

If the certificate is self-signed by the device, additional operations on the remote station's certificate must be performed as listed below:

- Verify the certificate digital signature.
- Verify that the starting validity date permits the certificate to be used.
- Verify that the certificate is not expired.
- Verify that the public key contained in the received certificate is provisioned on the local station as described in 8.3.4.

8.3.8.3 Verification of certificate signed by the central authority

If the Central Authority is supported and the certificate is signed by the Central Authority, the following operations on the remote station's certificate must be performed as listed below (refer to IEC 62351-9 for certificate verification):

- Verify that the certificate was issued by a recognized Central Authority. The Certificates of the Central Authority shall be provisioned to the stations as described in 8.3.4.
- If an attribute certificate is received, verify that the corresponding ID certificate is provisioned to the local station.
- Verify the certificate digital signature.
- Verify that the starting validity date permits the certificate to be used.
- Verify that the certificate is not expired.
- Verify that the certificate is not revoked by the Central Authority.
- If RBAC and the Area of Responsibility (AoR) are supported, verify that the AoR text strings in the remote station's certificate matches at least one such string in the local station's certificate.
- Optionally, if the list of authorized remote stations is configured, verify the Distinguished Name of the certificates.

8.3.9 Verification of certificates during normal operations

Both controlling and controlled stations shall be able to verify the status of their own certificate as well as the remote station's certificate on regular basis during normal operations.

The local station should verify the expiration of its own certificate and the remote station's certificate at least every 24 hours.

Furthermore, if the Central Authority is supported and certificates signed by the Central Authority are used in the Station Association procedure, the local station should verify the revocation status of its own certificate as well as the remote station's certificate at least every 24 hours. The method to perform the certificate revocation check is out of scope of this document and should follow the directives defined in IEC 62351-9, other methods to verify the certificates revocation status may be defined in the affected protocol referencing standards.

If either local station's certificate or the remote station's certificate expires while the Update Keys are valid, the local station shall not invalidate the Update Keys.

If either local station's certificate or remote station's certificate is revoked by the Central Authority while the Update Keys are valid, the local station shall invalidate the Update Keys and the Session Keys of the associations established with that certificate.

The Central Authority shall provide a new certificate to each station before its certificate expires or is revoked. When a new certificate is provided to either the controlling station or the controlled station, the controlling station shall be solicited to initiate the Station Association procedure at the earliest opportunity.

8.3.10 Update Keys derivation

Both controlling and controlled stations shall generate the Update Keys as described in 8.3.10.

The controlling station derives the Update Keys after receiving the Association Response message from the controlled station and generating the random data for the Update key Change Request message next to be sent. The controlled station derives the Update Keys when it receives an Update Key Change Request message.

The size of the Update Keys is 256 bits (32 octets) because the algorithms selected in KWA and MAL fields in the Update Key Change Request message, described in 8.3.5.4, require 256 bits sized keys. The devices shall derive the Update Keys according to RFC 5869:

1) Devices exchange their X.509 certificate and fresh generated random data during the Station Association procedure as described in 8.3.5.
2) Each device performs the same scalar multiplication function on its own private key and the public key of the other device to produce the Intermediate Keying Material IKM (K in RFC 7748).

   NOTE for each controlling station/controlled station connection, the value of IKM will not change unless either side changes its certificate/private key data.
3) Each device shall concatenate the Random Data exchanged, controlling station and controlled station random data in that order, to produce the Salt value.
4) Each device shall perform the HKDF-Extract (Salt, IKM) function to produce the Pseudo-Random Key (PRK)
5) Each device shall perform the HKDF-Expand (PRK, Info, L) function to produce a value T of L octets long. The value of the parameter L must be 64 so that 64 octets are generated as output by this function. The Info parameter shall be a zero-length string.
6) The first 32 octets of T, T[1], shall be the Encryption Update Key used to encrypt the Session Keys in the Session Key Change procedure described in 8.4.
7) The last 32 octets of T, T[2], shall be the Authentication Update Key used to calculate the MAC to authenticate the messages exchanged in the Station Association procedure currently running, described in 8.3, as well as in the subsequent Session Key Change procedures performed, described in 8.4.

The derived Update Keys and the corresponding Association ID 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.

8.3.11 Controlling station directives for Station Association and Update Keys management

The controlling station shall initiate the Station Association procedure at the earliest opportunity when the communication with the controlled station is established if the Update Keys are not initialized or not valid, or when it is requested by the Central Authority or by the application.

If the Station Association procedure fails, the controlling station shall not retry the procedure automatically: the controlling station shall notify the failure to the organization so that the authorized personnel can take the appropriate actions. The possible methods to notify a Station Association failure are described in 7.5.

If the current Update Keys are valid, the controlling station shall not invalidate the Update Keys when it initiates a new Station Association procedure or when that procedure fails. Instead, the controlling station shall consider the current Update Keys still valid until the next Station Association procedure has been successfully completed (i.e. the controlling station receives a valid Update Key Change Response message). Each time a Station Association procedure has been successfully completed the controlling station shall use the newly generated Update Keys to change the Session Keys in all the subsequent Session Key Change procedures as described in 8.4.

8.3.12 Controlled station directives for Station Association and Update Keys management

8.3.12.1 General

The controlled station shall await the controlling station to initiate the Station Association procedure if the Update Keys are not initialized or not valid.

Optionally, the controlled station may solicit the controlling station to initiate a Station Association procedure by sending an Association Initiation Request message to the controlling station as described in 8.3.5.6.

If the current Update Keys are valid, the controlled station shall not invalidate the Update Keys when it receives an Association Request message from the controlling station or when the Station Association procedure fails. Instead, the controlled station shall consider the current Update Keys still valid until it receives a valid Update Key Change Request message from the controlling station, then it shall generate and use the new Update Keys to change the Session Keys in all the subsequent Session Key Change procedures, as described in 8.4.

It is strongly recommended the controlled station to limit the number of concurrent associations supported. The outstation is permitted to not respond to any Association Request if this limit is exceeded.

8.3.12.2 Role-Based Access Control (RBAC) management on controlled station

8.3.12.2.1 General

The support of RBAC mechanism is optional. If the controlled station support RBAC mechanism, it shall be implemented as described in 8.3.12.2.

On the controlled station, each controlling station authorized to communicate has roles and permissions associated to it. The Role of the controlling station shall determine what actions it is allowed to perform on the controlled station. Table 17 describes the minimum set of standard roles and the corresponding permissions to be supported. These roles are aligned with those defined in IEC 62351-8, the permissions are specific to this standard. Implementations may introduce additional roles and permissions on the private range as defined in IEC 62351-8. The mechanism to provide additional defined roles is described in IEC 62351-8. *RoleDefinition* is a mandatory field and shall be set to IEC 62351-5 for roles defined in this document. *Revision* is also a mandatory field and shall be set to 0. The *RoleDefinition* and *Revision* are part of the access token defined in IEC 62351-8.

Table 17 – List of pre-defined role-to-permission assignment

Value	Permission / Role Name	MONITOR DATA	OPERATE CONTROLS	FILEREAD	FILEWRITE	FILEMNGT	CONFIG OPERATION PARAMETERS	CONFIG SECURITY PARAMETERS
<0>	VIEWER	X		C_1				
<1>	OPERATOR	X	X	C_1				
<2>	ENGINEER	X		X_1	X_1	X_1	X	
<3>	INSTALLER	X		X_2	X_2		X	
<4>	SECADM			X_4	X_4	X_4		X
<5>	SECAUD			X_3				
<6>	RBACMNT			X_4	X_4	X_4		X
<7…32767>	Reserved	For future use of IEC defined roles.						
<-32768…-1>	Private	Defined by external agreement. Not guaranteed to be interoperable.						

C_1 Conditional read access to files of filetype data (may not access security settings, but process values)

X_1 Access to files of type data and config

X_2 Access to files of type config and firmware (updates)

X_3 Access to files of type audit log

X_4 Access to files of type security (config)

8.3.12.2.2 RBAC using self-signed certificates

If self-signed certificates are used in the Station Association procedure, the controlled station shall permit the RBAC information to be pre-configured for each controlling station authorized to communicate as described in 8.3.2.3. This configuration shall be permitted only to authorized personnel. The method to configure RBAC information on devices is out of scope of this document.

If self-signed certificate contains RBAC information, the controlled station shall ignore that information.

8.3.12.2.3 RBAC using certificate signed by a Central Authority

If the Central Authority is supported and the certificates signed by the Central Authority are used in the Station Association procedure, the controlled station shall be able to retrieve and store the controlling station Roles from the RBAC extension in the controlling station's certificate.

Upon receiving the controlling station's public key certificate, if the public key certificate does not contain RBAC information, the controlled station may optionally fetch controlling station's attribute certificate containing RBAC information from an external repository. The method to retrieve the attribute certificate from such repository (PULL method) is described in IEC 62351-8.

For each Association ID, the controlling station's RBAC information shall be stored permanently on the controlled station each time the Station Association procedure has been successfully executed, so that that information will be maintained after a station initialization or after a communication failure.

8.3.13 Initializing and updating Stations Association and Update Keys

Figure 6 illustrates the initialization of the Association ID and the corresponding Update Keys, followed by the initialization of the corresponding Session Keys during the enrolment of a device or whenever the Station Association procedure is required.

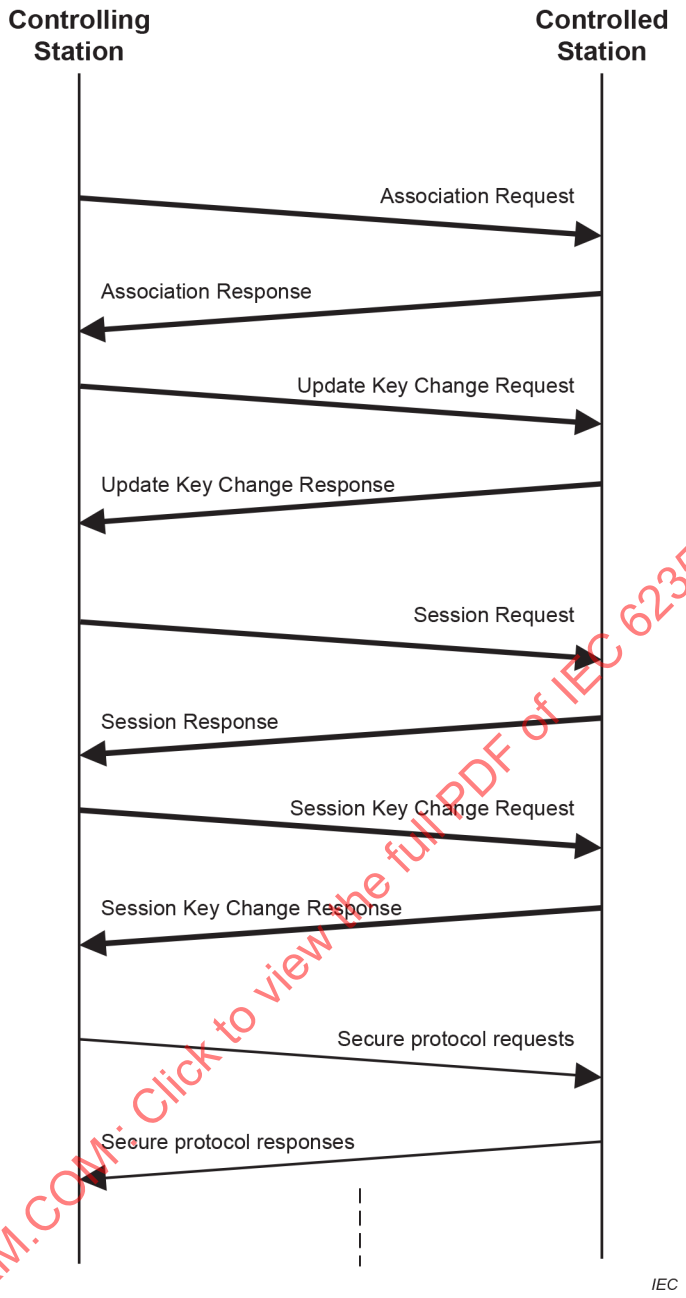


Figure 6 – Example of Association ID, Update Keys and Session Keys initialization

8.4 Session Key Change procedure

8.4.1 General

This procedure shall be performed to initialize or renew the Session keys for an Association. Each device shall maintain a unique set of Session Keys for each controlling station/controlled station association established during the Station Association procedure.

This procedure can be performed only if both controlling and controlled stations own the Update Keys corresponding to the Association ID.

8.4.2 Messages definition

8.4.2.1 General

Subclause 8.4.2 describes security messages and data exchanged in each security message executing the Session Key Change procedure. Figure 7 illustrates the messages and data exchanged in detail.

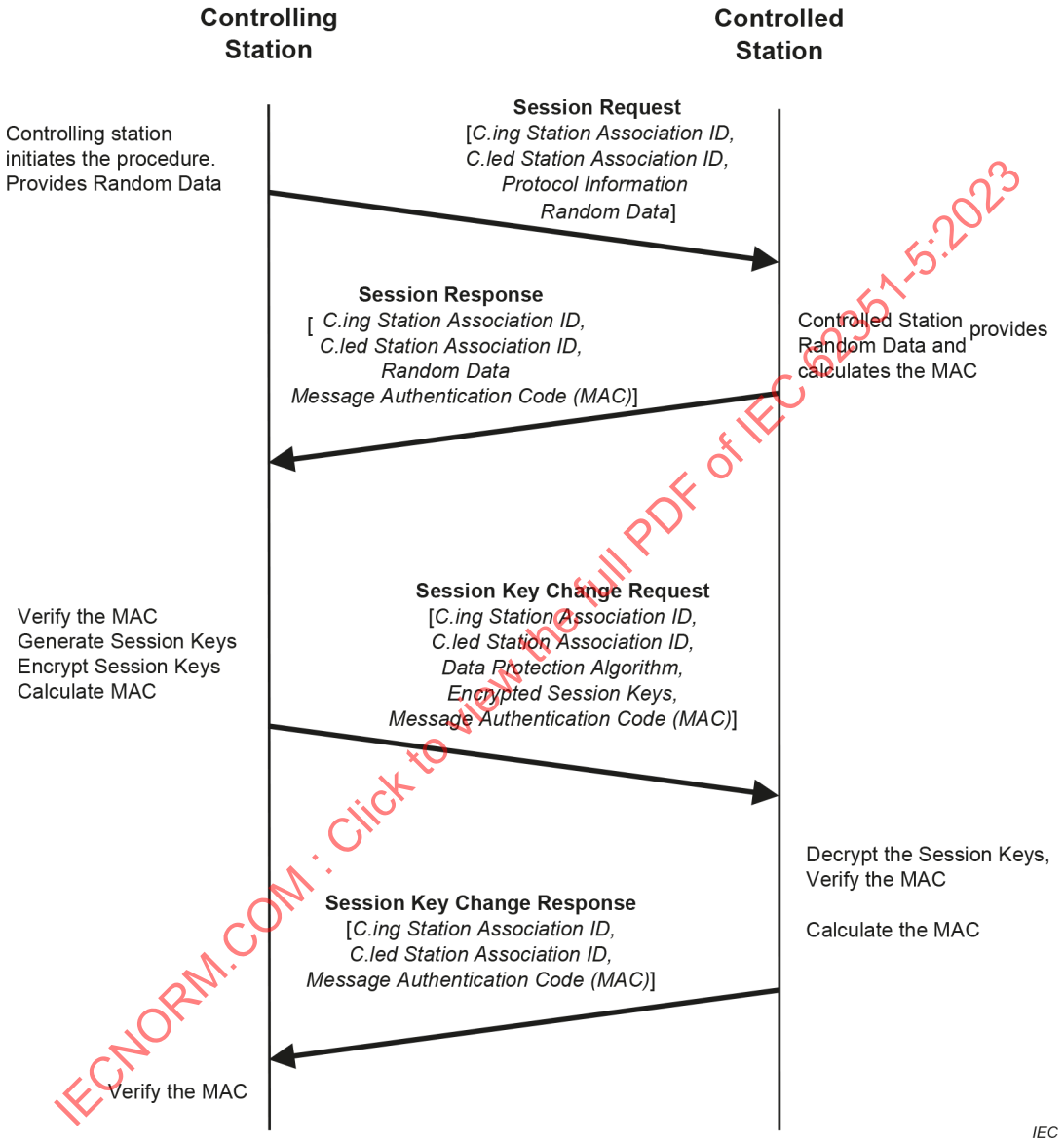


Figure 7 – Session Key Change procedure

8.4.2.2 Session Request message

8.4.2.2.1 Structure

Each Session Request message shall contain the information described in 8.4.2.2 and summarized in Table 18.

The controlling station (only) shall send the Session Request message. Through this message the controlling station initiates the Session Key Change procedure. The Session Request message shall elicit a Session Response message from the controlled station.

After sending the Session Request message, the controlling station shall start the Reply Timer to verify that the Session 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 indicated in the corresponding state machine described in 8.4.3.

Table 18 – Session Request message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Value Value	PRI = Protocol Information

Value	CGL = Controlling station random data length
Number of octets specified in CGL	CGD = Controlling station random data

8.4.2.2.2 Controlling station Association ID

This is the value the controlling station has chosen to represent the communication link with this controlled station. This value shall match the AIM in the last Update Key Change Request sent to the controlled station during the successful Station Association procedure most recently performed for this communication link, described in 8.3.5.4.

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

8.4.2.2.3 Controlled station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. This value shall match the AIS in the last Update Key Change Response received by the controlled station during the successful Station Association procedure most recently performed for this communication link, described in 8.3.5.5.

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

8.4.2.2.4 Protocol Information

The controlling station uses this field to provide protocol information, including the protocol version, it intends to use to the controlled station.

The structure and the possible values in this field shall be specified by the affected protocol referencing standards.

Controlling and controlled stations may support multiple protocol versions. The controlled station shall validate the Protocol Information value specified in the Session Request message received, the rules to validate the Protocol Information value on the controlled station must be specified in the affected protocol referencing standards. If the Protocol Information value is considered not valid in the referencing standard, the controlled station shall ignore the Session Request received.

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

8.4.2.2.5 Controlling Station Random Data Length

This value shall specify the length in octets of the random data that follows. The minimum length of the random data in this message shall be four octets, the maximum length is 64 octets.

CGL:= UI8[1..8]<4..64>

8.4.2.2.6 Controlling Station Random Data

The controlling station shall include this random data in the Session Request message to ensure that the contents of the subsequent Session Response message are not predictable and to protect the controlling station against replay attacks. The random data shall be generated using the algorithm specified in NIST SP 800-90A Rev.1.

CGD:= OS8i[1..8i]; i:=CGL

8.4.2.3 Session Response message

8.4.2.3.1 Structure

Each Session Response message shall contain the information described in 8.4.2.3 and summarized in Table 19.

The controlled station (only) shall send the Session Response message each time a Session Request message is received from the controlling station.

The Session Response provides random data that the controlling station must use to authenticate the subsequent Session Key Change Request message.

After sending the Session Response message, the controlled station shall start the Request Timer to verify that the subsequent Session Key Change Request message is received from the controlling station within the expected time. If the Request Timer expires (Request Timeout), the controlled station shall execute the actions indicated in the corresponding state machine described in 8.4.4.

The Request Timer shall be stopped when a valid Session Key Change Request message is received.

Table 19 – Session Response message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Value	CGL = Controlled station random data length
Number of octets specified in CGD	CGD = Controlled station random data
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, defined in 8.3.5.4.5	MAC = Message authentication code

8.4.2.3.2 Controlling station Association ID

This value shall match the AIM in the Session Request message most recently received from the controlling station, described in 8.4.2.2.2.

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

8.4.2.3.3 Controlled station Association ID

This value shall match the AIS in the Session Request message most recently received from the controlling station, described in 8.4.2.2.3.

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

8.4.2.3.4 Station Random Data Length

This value shall specify the length in octets of the random data that follows. The minimum length of the random data in this message shall be four octets, the maximum length is 64 octets.

CGL:= UI8[1..8]<4..64>

8.4.2.3.5 Controlled station random data

The controlled station shall include this random data in the Session Response message to ensure that the contents of the subsequent Session Key Change Request message are not predictable and to protect the controlled station against replay attacks.

Random number generators are responsible for providing statistically adequate random data. Guidance for random number generation can be found in NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C as well as in IETF RFC 4086

CGD:= OS8i[1..8i]; i:=CGL

8.4.2.3.6 Message Authentication Code

The controlled station shall use this field to authenticate the data included in Session Response message being transmitted.

This value shall be calculated using the MAC algorithm selected in Update Key Change Request message, described in 8.3.5.4.5, using the corresponding **Authentication Update Key** generated as described in 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 20, referencing standards may require further information, in addition to those indicated in Table 20, to be included in the MAC calculation. The length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.3.5.4.5.

Table 20 – Data Included in MAC calculation (in order)

Data	Description	Described in	Source
Session Request values	The entire Session Request message most recently received.	Subclause 8.4.2.2	Session Request
Session Response values	The entire Session Response message being transmitted up to and including CGD (excluding the MAC field).	Subclause 8.4.2.3	Session Response
Padding data	Additional padding data required by the MAC algorithm.	Algorithm specification.	Required by algorithm.

MAC:= OS8i[1..8i]; i:=as specified in MAL of this message, defined in 8.3.5.4.5.

8.4.2.4 Session Key Change Request message

8.4.2.4.1 Structure

Each Session Key Change Request message shall contain the information described in 8.4.2.4 and summarized in Table 20.

Only the controlling station shall send Session Key Change Request messages. A Session Key Change Request message shall be a notice from the controlling station of a change in the Session Keys and shall elicit a Session Key Change Response message from the controlled station.

After sending the Session Key Change Request message, the controlling station shall start the Reply Timer to verify that the Session Key Change 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 indicated in the state machine described in 8.4.3.

Table 21 – Session Key Change Request message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Enumerated value	DPA = Data protection algorithm
Value Value	WKL = Wrapped key data length
Number of octets specified in WKL	WKD = Wrapped key data
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5	MAC = Message authentication code

8.4.2.4.2 Controlling station Association ID

This is the value that the controlling station has chosen to represent the communication link with this controlled station. This value shall match the AIM provided in the Session Request most recently transmitted to the controlled station, described in 8.4.2.2.2.

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

8.4.2.4.3 Controlled station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. This value shall match the AIS provided in the Session Request most recently transmitted to the controlled station, described in 8.4.2.2.3.

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

8.4.2.4.4 Data Protection Algorithm

Using this value, the controlling station shall indicate to the controlled station the selected algorithm to encrypt or authenticate the application data in the Secure Data messages exchanged, described in 8.5, after the current Session Key Change procedure has been successfully terminated.

The encryption and authentication algorithms mandatory to be supported are listed in Clause 9: Interoperability Requirements. The best available option should be selected in this field.

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

<0>:= reserved

<1>:= reserved

<2>:= obsoleted

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

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

<5>:= obsoleted

<6>:= obsoleted

<7>:= HMAC-SHA3-256 truncated to 8 octets (serial)

<8>:= HMAC-SHA3-256 truncated to 16 octets (networked)

<9>:= BLAKE2s-256 truncated to 8 octets (serial)

<10>:= BLAKE2s-256 truncated to 16 octets (networked)

<11>:= AEAD-AES-256-GCM encryption (serial and networked)

<12..127>:= reserved for future use

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

8.4.2.4.5 Wrapped Key Data Length

This value shall be the length of the data produced by the key wrap algorithm, as described in 8.4.2.4.6. Note that AES-256 algorithm used to wrap the Session Keys generates 64 octets output at minimum with a session key length of 256 bits.

WKL:= UI16[1..16]<64 ..65535>

8.4.2.4.6 Wrapped Key Data

The controlling station shall use this value to provide the Session Keys to the controlled station.

This value shall be obtained executing the key wrap algorithm selected during the last Station Association procedure successfully performed for this Association, described in 8.3.5.4.4, using the corresponding Encryption Update Key generated as described in 8.3.10.

The controlling station shall pass the data through the Key Wrap Algorithm in the order described in Table 21.

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

Table 22 – Data Included in WKD (in order)

Data	Description	Described in	Source
Control Direction Session Key	The key used to authenticate data from the controlling station.	Table 2	Generated by the controlling station
Monitoring Direction Session Key	The key used to authenticate data from the controlled station.	Table 2	Generated by the controlling station
Padding data	As required by the key wrap algorithm.	Algorithm specification.	Required by algorithm.

The length of the Session Keys shall be 256 bits (32 octets).) because the algorithm selected in DPA field in the Session Key Change Request message, described in 8.4.2.4.4, requires a 256 bits sized key. The Session Key generators are responsible for providing statistically adequate random data. Guidance for random number generation can be found in NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C as well as in IETF RFC 4086.

The Session Keys shall be treated as arrays of octets and transmitted with the lowest index octet first. For example, Appendix A of the AES specification FIPS PUB 197 provides the example of a 256-bit cipher key shown in Table 22. The byte with index 0, having value 2B, shall be transmitted first as indicated in Table 22.

Table 23 – Example of Session Key order

Value	60	3D	EB	10	15	CA	71	BE	2B	73	AE	F0		14	DF	F4
Index	0	1	2	3	4	5	6	7	8	9	10	11		29	30	31
NOTE The output from the key wrap algorithm could be longer than the input. For instance, the AES Key Wrap Algorithm produces output that is exactly 8 octets longer than its input.																

8.4.2.4.7 Message Authentication Code

The controlling station shall use this value to authenticate the data included in Session Key Change Request message being transmitted.

This value shall be calculated using the MAC algorithm selected during the last Station Association procedure successfully performed for this communication link, described in 8.3.5.3.5, using the corresponding Authentication Update Key generated as described in 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 23, the, referencing standards may require further information, in addition to those indicated in Table 23, to be included in the MAC calculation. the length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.3.5.3.5.

Table 24 – Data Included in the MAC calculation (in order)

Data	Description	Described in	Source
Controlled station Random data	The random data provided in the Session Response most recently received from the controlled station.	Subclause 8.4.2.3.5	Session Response
Session Key Change Request values	The entire Session Key Change Request message being transmitted up to and including WKD (excluding the MAC field).	Subclause 8.4.2.4	Session Key Change Request
Padding data	As required by the MAC algorithm.	Algorithm specification.	Required by algorithm.

MAC:= OS8i[1..8i]; i:=as specified in MAL of the Update Key Change Request message most recently received, described in 8.3.5.3.5.

8.4.2.5 Session Key Change Response message

8.4.2.5.1 Structure

Each Session Key Change Response message shall contain the information described in 8.4.2.4 and summarized in Table 24.

The controlled station (only) shall send Session Key Change Response messages whenever a valid Session Key Change Request message is received from the controlling station. Through this message the controlled station confirms to the controlling station the possession of the new Session keys and concludes the Session Key Change procedure.

Table 25 – Session Key Change Response message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5	MAC = Message authentication code

8.4.2.5.2 Controlling station Association ID

This value shall match the AIM in the Session Key Change Request message most recently received from the controlling station, described in 8.4.2.4.2.

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

8.4.2.5.3 Controlled station Association ID

This value shall match the AIS in the Session Key Change Request message most recently received from the controlling station, described in 8.4.2.4.3.

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

8.4.2.5.4 Message Authentication Code

The controlled station shall use this value to authenticate the data included in Session Key Change Response message being transmitted.

This value shall be calculated using the MAC algorithm selected during the last Station Association procedure successfully performed for this Association, described in 8.3.5.4.5, using the corresponding Authentication Update Key generated as described in 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 26, referencing standards may require further information, in addition to those indicated Table 26, to be included in the MAC calculation. The length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.3.5.4.5.

Table 26 – Data Included in the MAC calculation (in order)

Data	Description	Described in	Source
Session Key Change Request values	The entire Session Key Change Request message most recently received from the controlling station.	Subclause 8.4.2.4	Session Key Change Request
Session Key Change Response values	The entire Session Key Change Response message being transmitted up to and including AIS (excluding the MAC field).	Subclause 8.4.2.5	Session Key Change Response
Padding data	As required by the MAC algorithm.	Algorithm specification.	Required by algorithm.

MAC:= OS8i[1..8i]; i:=as specified in MAL of the Update Key Change Request message most recently received, defined in 8.3.5.4.5.

8.4.2.6 Session Key Change Procedure solicited by the controlled station

If spontaneous unsolicited messages from the controlled station are permitted, the controlled station may optionally solicit the controlling station to initiate the Session Key Change procedure by sending a Session Initiation Request message. The affected protocol referencing standards may define the Session Initiation Request message and its management.

8.4.3 Controlling station state machine

On the controlling station, the Session Key Change messages described in 8.4.2 shall be managed by the state machine described in 8.4.3. Figure 8 illustrates an overview (informative) of the Session Key Change transactions on the controlling station. The controlling station shall execute the Session Key Change state machine described in Table 27 (normative). The *Key Management Idle* state is shared (in common) with the Station Association state machine.

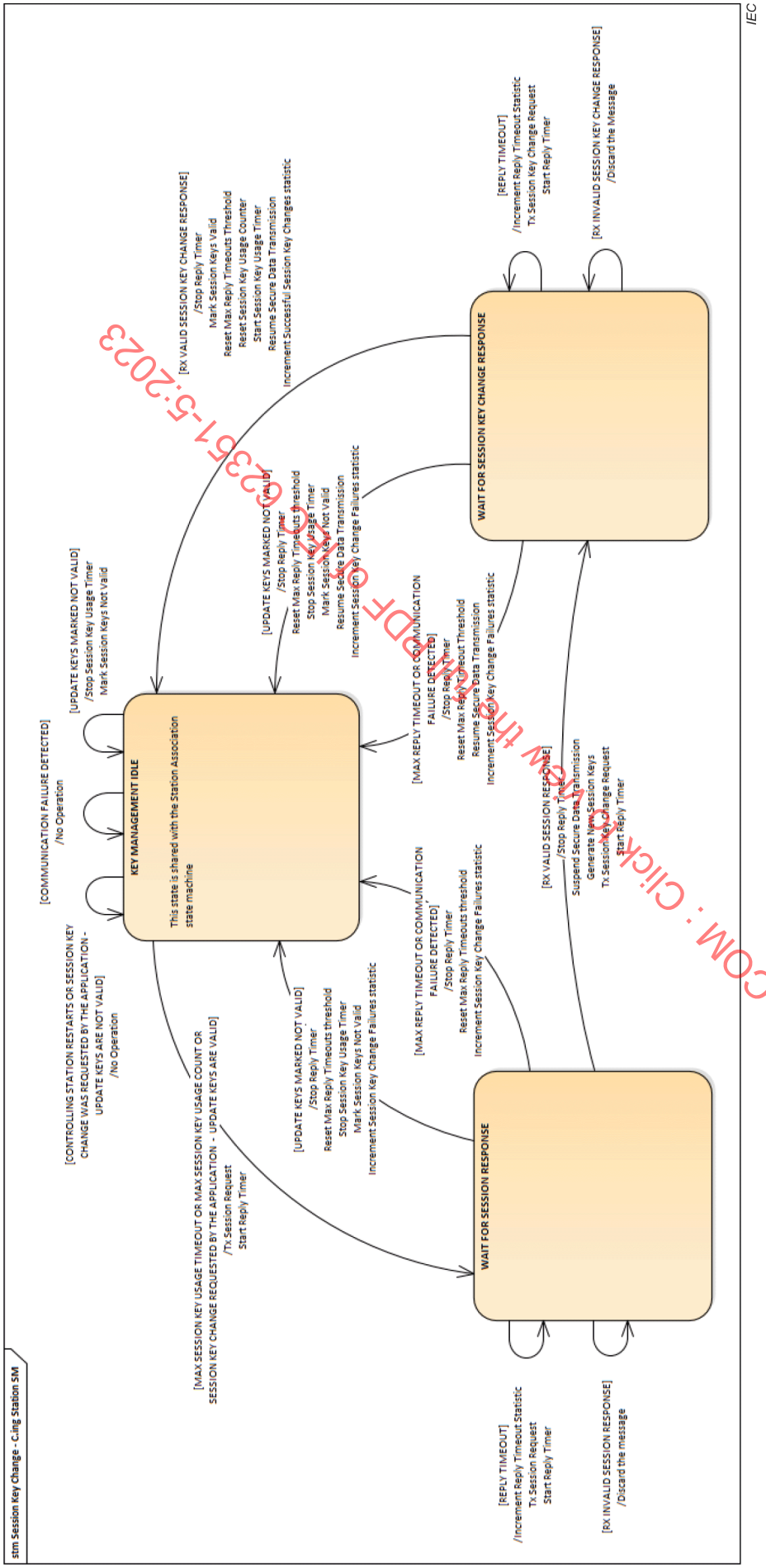


Figure 8 – Session Key Change – Controlling station state machine

Table 27 – Controlling station state machine: Session Key Change

Event	Event Description	State						
		Key Management Idle (this state is shared with the Station Association state machine)		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Session Key Usage Time expired	The Session Key Usage Time has expired.	Transmit the Session Request message. Start the Reply Timer.	Wait for Session Response	No Operation (This event shall be managed in the "*Key Management Idle*" state)	Wait for Session Response	No Operation (This event shall be managed in the "*Key Management Idle*" state)	Wait for Session Key Change Response	**1**
Session Key Usage Count exceeded	Number of times the session key has been used has exceeded the Max Session Key Usage Count threshold.	Transmit the Session Request message. Start the Reply Timer.	Wait for Session Response	No Operation (This condition shall be checked when the state machine is in the "*Key Management Idle*" state)	Wait for Session Response	No Operation (This condition shall be checked when the state machine is in the "*Key Management Idle*" state)	Wait for Session Key Change Response	**2**
Session Key Change requested by the application	The application has requested to perform the Session Key Change procedure.	IF the Update Keys are Valid: Transmit the Session Request message. Start the Reply Timer.	Wait for Session Response	Discard the event. (The controlling station is already executing the procedure in this state)	Wait for Session Response	Discard the event. (The controlling station is already executing the procedure in this state)	Wait for Session Key Change Response	**3**
		IF the Update Keys are Not Valid: No Operation	Key Management Idle					

Event	Event Description	State						
		Key Management Idle (this state is shared with the Station Association state machine)		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Valid Session Response	The controlling station has received a Session Response with valid parameters.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Stop Reply Timer Suspend the secure data transmission in the Secure Data Exchange state machine Generate the new Session Keys Transmit the Session Key Change Request message. Start the Reply Timer.	Wait for Session Key Change Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Response	**4**
Rx Invalid Session Response: the message is not authentic	The controlling station has received a Session Response message with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the Authentication Errors statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Response	**5**

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Station Association state machine)**		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Session Response the message contains parameter error(s)	The controlling station has received Session Response with one of the following conditions a) The controlling station Association ID does not match that in the Session Request b) The controlled station Association ID does not match that in the Session Request c) The Random Data Length is less than minimum required d) The Random Data Length is over the maximum allowed	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Response	Increment the Unexpected Messages statistic. Discard the message. Increment the Discarded Messages statistic.	Wait for Session Key Change ResponseKey	6

Event	Event Description	State						
		Key Management Idle (this state is shared with the Station Association state machine)		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Valid Session Key Change Response	The controlling station has received a correctly authenticated Session Key Change Response with valid parameters.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic. (This event should not be possible, since the MAC cannot be valid until the controlling station sends a Session Key Change Request message and, in that case, the controlling station would be in Wait for Session Key Change Response state)	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic. (This event should not be possible, since the MAC cannot be valid until the controlling station sends a Session Key Change Request message and, in that case, the controlling station would be in Wait for Session Key Change Response state)	Wait for Session Response	Stop Reply Timer. Mark Session Keys as Valid. Start the Session Key Usage timer Reset the Session Key Usage counter. Reset Max Reply Timeouts threshold Reset the Data Sequence Number (DSQ) Resume the secure data transmission in the Secure Data Exchange state machine Increment *Successful Session Key Changes* statistic.	Key Management Idle	7
Rx Invalid Session Key Change Response: the message is not authentic.	The Controlling Station received a Session Key Change Response message with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Response	Increment the *Key Authentication Errors* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Response	8

Event	Event Description	State						
		Key Management Idle (this state is shared with the Station Association state machine)		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Rx Invalid Session Key Change Response: the message contains parameter error(s)	The controlling station received a correctly authenticated Session Key Change Response with one of the following error conditions: a) The Controlling Station Association ID does not match that in the Session Request The Controlled Station Association ID does not match that in the Session Request.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Key Management Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Response	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Response	**9**
Reply Timeout	The Reply Timer has expired while the controlling station was waiting for a response from the controlled station and the Reply Timeouts statistic has not reached the Max Reply Timeouts threshold	Discard the event. (This event can occur only when the state machine is in the "*Wait for Session Response*" state or in the "*Wait for Session Key Change Response*" state)	Key Management Idle	Increment the *Reply Timeouts* statistic. Transmit the Session Request message Start the Reply Timer.	Wait for Session Response	Increment the *Reply Timeouts* statistic. Re-transmit the last Session Key Change Request message transmitted Start the Reply Timer.	Wait for Session Key Change Response	**10**

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Station Association state machine)**		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Max Reply Timeouts	The current Session Key Change procedure has failed because the Reply Timeout statistic has reached Max Reply Timeouts threshold while the controlling station was waiting for a response from the controlled station.	Discard the event. **(This event can occur only when the state machine is in the "*Wait for Session Response*" state or in the "*Wait for Session Key Change Response*" state)**	Key Management Idle	Increment the Max *Reply Timeouts* statistic. Reset Max Reply Timeouts threshold. Increment the *Session Key Change Failures* statistic	Key Management Idle	Increment the Max *Reply Timeouts* statistic. Reset Max Reply Timeouts threshold. Resume the secure data transmission in the Secure Data Exchange State Machine Increment the *Session Key Change Failures* statistic	Key Management Idle	**11**
Controlling station Initialization.	The controlling station has initialized or restarted.	IF the Update Keys are Valid: – Transmit the Session Request message. – Start the Reply Timer.	Wait for Session Response	IF the Update Keys are Valid: – Transmit the Session Request message. – Start the Reply Timer.	Wait for Session Response	IF the Update Keys are Valid: – Transmit the Session Request message. – Start the Reply Timer.	Wait for Session Response	**12**
		IF the Update Keys are Not Valid: – No Operation	Key Management Idle	IF the Update Keys are Not Valid: – No Operation	Key Management Idle	IF the Update Keys are Not Valid: – No Operation	Key Management Idle	

Event	Event Description	State						
		Key Management Idle **(this state is shared with the Station Association state machine)**		**Wait for Session Response**		**Wait for Session Key Change Response**		
		Stable state to manage Session Keys and Update Keys		The controlling station is waiting for the controlled station to send the response to the Session Request message		The controlling station is waiting for the controlled station to send the response to the Session Keys Change Request message.		
		Action	**Next State**	**Action**	**Next State**	**Action**	**Next State**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Communication Failure Detected Note: this event shall be considered if communication failures can be detected in the communication link.	The station has detected a communication failure.	No Operation.	Key Management Idle	Stop Reply Timer. Reset Max Reply Timeouts threshold Increment the *Session Key Change Failures* statistic.	Key Management Idle	Stop Reply Timer. Reset Max Reply Timeouts threshold Resume the secure data transmission in the Secure Data Exchange state machine Increment the *Session Key Change Failures* statistic.	Key Management Idle	**13**
Update Keys Marked Not Valid.	The Update Keys were marked Not Valid by the Station Association state machine.	Stop Session Key Usage Timer Reset Session Key Usage Counter Mark Session Keys as Not Valid	Key Management Idle	Stop Reply Timer Reset Max Reply Timeouts threshold Mark Session Keys as Not Valid Stop Session Key Usage Timer Reset Session Key Usage Counter Increment the Session Key Change Failures statistic.	Key Management Idle	Stop Reply Timer Reset Max Reply Timeouts threshold Mark Session Keys as Not Valid Stop Session Key Usage Timer Reset Session Key Usage Counter Resume the secure data transmission in the Secure Data Exchange state machine Increment the Session Key Change Failures statistic.	Key Management Idle	**14**

8.4.4 Controlled station state machine

On the controlled station, the Session Key Change messages described in 8.4.2 shall be managed by the state machine described in 8.4.4. Figure 9 illustrates an overview (informative) of the Session Key Change transactions on the controlled station. The controlled station shall execute the Session Key Change state machine described in Table 28 (normative).

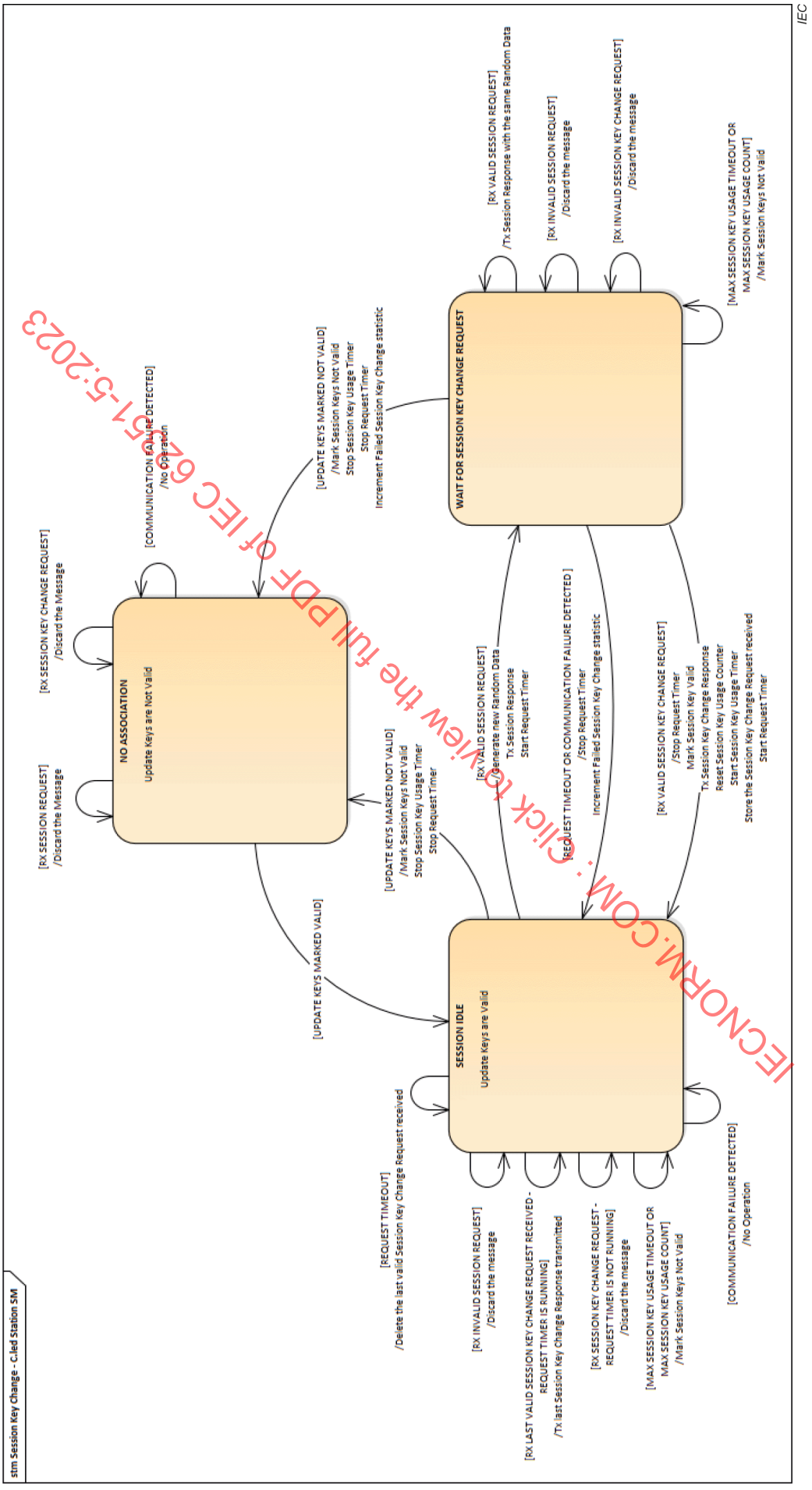


Figure 9 – Session Key Change – Controlled station state machine

Table 28 – Controlled station state machine: Session Key Change

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Rx Valid Session Request	The controlled station has received a valid Session Request.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Generate new random data to be transmitted. Transmit the session Response with the new random data generated. Start Request Timer	Wait for Session Key Change Request	Transmit the session Response with the same random data provided in the last session Response transmitted	Wait for Session Key Change Request	1
Rx Invalid Session Request: Protocol Information Error.	The controlled station receives a Session Request specifying a Protocol Information value not permitted or not supported	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Increment the *Protocol Information Errors* statistic Discard the message Increment the *Discarded Messages* statistic.	Session Idle	Increment the *Protocol Information Errors* statistic Discard the message Increment the *Discarded Messages* statistic.	Wait for Session Key Change Request	2

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Rx Invalid Session Request: the message contains parameter error(s)	The controlled station has received a Session Request with one of the following error conditions: a) The controlling station Association ID is incorrect. b) The controlled station Association ID is incorrect. c) The Random Data Length is less than the minimum required d) The Random Data Length is over the maximum allowed	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Request	3

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Rx Valid Session Key Change Request	The controlled station has received a correctly authenticated Session Key Change Request with valid parameters.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	IF Request Timer is running AND the Session Key Change Request is identical to last valid Session Key Change Request received: –Retransmit the Session Key Change Response most recently transmitted ELSE: –Increment the *Unexpected Messages* statistic. –Discard the message. –Increment the *Discarded Messages* statistic	Session Idle	Stop Request Timer Transmit the Session Key Change Response Mark Session Key as Valid. Start the Session Key Usage timer Reset the Session Key Usage counter. Reset the Data Sequence Number (DSQ). Store the Session Key Change Request received Start Request Timer. Increment the *Successful Session Key Changes* statistic	Session Idle	4
Rx Invalid Session Key Change Request: the message is not authentic.	The controlled station received a Session Key Change Request with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Idle	Increment the *Key Authentication Errors* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Request	5

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Rx Invalid Session Key Change Request: the message contains parameter error(s)	The controlled station receives a correctly authenticated Session Key Change Request with one of the following error conditions: a) The Controlling station Association ID does not match that in the last Session Response transmitted b) The controlled station Association ID does not match that in the last Session Response transmitted	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Idle	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Request	6
Rx Invalid Session Key Change Request: Data Protection Algorithm is not permitted.	The controlled station receives a correctly authenticated Session Key Change Request specifying a Data Protection Algorithm (DPA) that is not permitted or not supported.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Association	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Idle	Increment the *Data Protection Algorithm Support Failures* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Wait for Session Key Change Request	7

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Request Timeout	The Request Timer has expired while the controlled station was waiting for a valid Session Key Change Request from the controlling station.	Discard the event. (This event can occur only when the state machine is in the "*Session Idle*" state or in "*Wait for Session Key Change Request*" state)	No Association	Delete the last valid Session Key Change Request received.	Session Idle	Increment the *Request Timeouts* statistic. Increment the *Session Key Change Failures* statistic.	Session Idle	8
Session Key Usage Time Expired	The controlled station has not received a valid Session Key Change Request message before that the Session Key Usage Time has expired.	Discard the event. (This event can occur only when the state machine is in the "*Session Idle*" state or in the "*Wait for Session Key Change Request*" state)	No Association	Mark Session Keys as Not Valid Increment the *Session Key Invalidations due to Usage Timeout* statistic	Session Idle	Mark Session Keys as Not Valid Increment the *Session Key Invalidations due to Usage Timeout* statistic	Wait for Session Key Change Request	9
Expected Session Key Usage Count Exceeded	The controlled station has not received a valid Session Key Change Request message before that the Session Key Usage Count has exceeded.	Discard the event. (This event can occur only when the state machine is in the "*Session Idle*" state or in the "*Wait for Session Key Change Request*" state)	No Association	Mark Session Keys as Not Valid Stop Session Key Usage Timer Increment the *Session Key Invalidations due to Usage Count* statistic	Session Idle	Mark Session Keys as Not Valid Stop Session Key Usage Timer Increment the *Session Key Invalidations due to Usage Count* statistic	Wait for Session Key Change Request	10

Event	Event Description	State						
		No Association		Session Idle		Wait for Session Key Change Request		
		Update Keys are NOT Valid		Update Keys are Valid		The controlled station is waiting for a Session Key Change Request from the controlling station		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Communication Failure Detected Note: this event shall be considered if communication failures can be detected in the communication link	The station has detected a communication failure.	No Operation.	No Association	No Operation.	Session Idle	Stop Request Timer. Increment the *Session Key Change Failures* statistic.	Session Idle	11
Update Keys Marked Valid.	The Update Keys were marked Valid by the Association state machine.	No further operation is required other than changing to the “Session Idle” state.	Session Idle	Discard the event. (This event can occur only when the state machine is in the “No Association” state)	Session Idle	Discard the event. (This event can occur only when the state machine is in the “No Association” state)	Wait for Session Key Change Request	12
Update Keys Marked Not Valid.	The Update Keys were marked Not Valid by the Association state machine.	Discard the event. (This event can occur only when the state machine is in the “Session Idle” state or in the “Wait for Session Key Change Request” state)	No Association	Mark Session Keys as Not Valid Stop Session Key Usage Timer Stop Request Timer	No Association	Mark Session Keys as Not Valid Stop Session Key Usage Timer Stop Request Timer Increment the Session Key Change Failures statistic	No Association	13

8.4.5 Controlling station directives for Session Keys management

The Session Keys can be initialized or changed only if the Update Keys are initialized (i.e. the Station Association procedure was successfully performed at least once since the controlling station's start-up). The controlling station cannot initiate a Session Key Change procedure if the Update Keys are not valid.

The controlling station shall initiate the Session Key Change procedure at the earliest opportunity under the following conditions:

– When the controlling station restarts
– After a successfully performed Station Association procedure
– When it is requested by the application.

The controlling station shall also periodically change the Session Keys each time one of the following events occur:

– The Session Keys Usage Timer has expired (Max Session Key Usage Time threshold).
– The Session Keys Usage Counter has reached the Max Session Key Usage Count threshold.

Max Session Keys Usage Time and Max Session Keys Usage Count thresholds shall be set using configurable parameters as discussed in 7.4.

The controlling station shall use the Encryption Update Key to wrap the Session Keys and transmit them to the controlled station in a Session Key Change Request message.

If the current Session Keys are valid, the controlling station shall not invalidate the Session Keys when it initiates a new Session Key Change procedure (i.e. when it sends a Session Request to the controlled station). Instead the controlling station shall consider the current Session Keys still valid until the next Session Key Change procedure has been successfully completed (i.e. the controlling station receives an authentic Session Key Change Response message). Each time a Session Key Change procedure has been successfully completed the controlling station shall use the new Session Key to authenticate and/or encrypt data in subsequent messages.

8.4.6 Controlled station directives for Session Keys management

The Session Keys can be initialized or changed only if the Update Keys are initialized (i.e. the Station Association procedure was successfully performed at least once since the controlled station's start-up). The controlled station shall only respond to Session Key Change procedure messages received by the controlling station if the Update Keys are valid.

Optionally, the controlled station may solicit the controlling station to initiate a Session Key Change procedure by sending a Session Initiation message to the controlling station as described in 8.4.2.5.

The controlled station shall use the Encryption Update Key to decrypt the Session Keys received from the controlling station in a Session Key Change Request message.

The controlled station shall also invalidate the Session Keys, as described in Table 27, each time one of the following events occur:

– The Session Keys Usage Timer has expired (Max Session Key Usage Time threshold).
– The Session Keys Usage Counter has reached the Max Session Key Usage Count threshold.

The Max Session Key Usage Time and Max Session Key Usage Count thresholds shall be set using a configurable parameter as described in 7.4.

In the controlled station, the Max Session Keys Usage Time and the Max Session Keys Usage Count thresholds shall be greater than the corresponding values set on the controlling station.

If the current Session Keys are valid, the controlled station shall not invalidate the Session Keys when it receives a Session Request message from the controlling station. Instead the controlled station shall consider the current Session Keys still valid until it receives an authentic Session Key Change Request message from the controlling station, then it shall use the new Session Keys received in this message to encrypt and authenticate data in subsequent messages.

8.4.7 Initializing and changing Session Keys

Figure 10 illustrates how the controlling station initializes and changes the Session Keys on start-up, periodically, and after a communications failure.

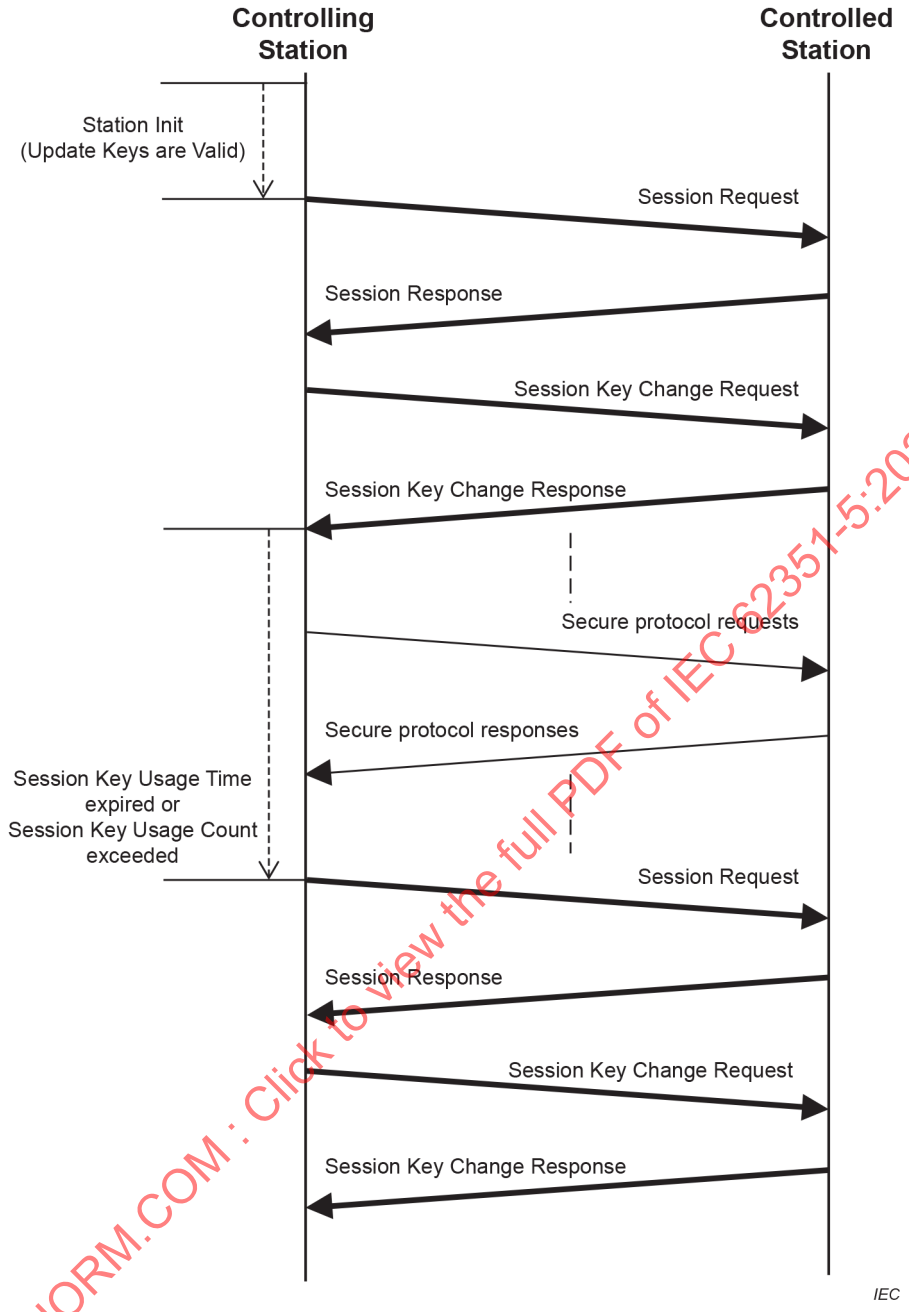


Figure 10 – Example of Session Key initialization and periodic update

8.5 Secure Data Exchange

8.5.1 General

The Secure Data Exchange is the normal operations procedure to authenticate and exchange application data between stations. It can be performed only if the Session Keys corresponding to the Association ID are valid in both controlling and controlled stations (after the Session Key Change procedure was successfully performed for that Association ID). Both controlling and controlled stations use the same operation and same message to authenticate and exchange application data.

8.5.2 Messages definition

8.5.2.1 General

Subclause 8.5.2 describes security messages and data exchanged in each security message executing the Secure Data Exchange. Figure 11 illustrates the messages and data exchanged in detail.

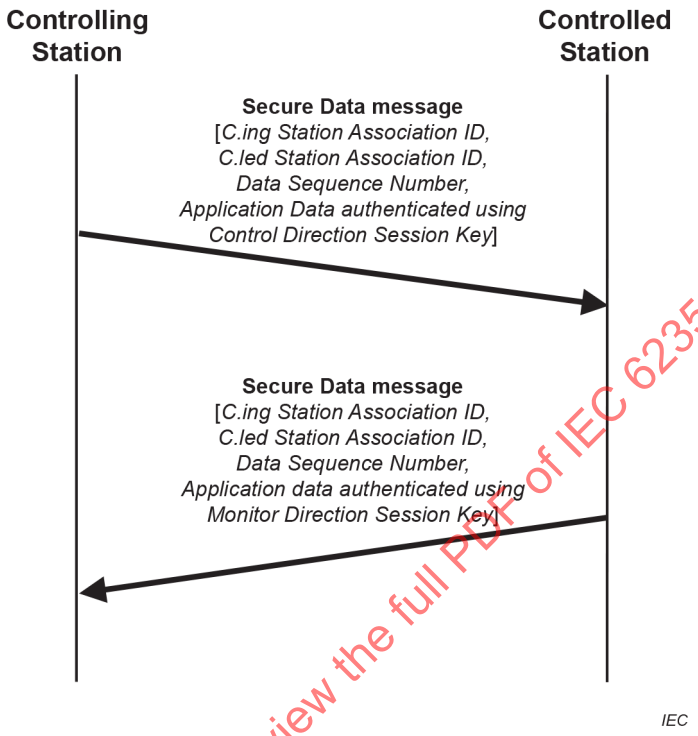


Figure 11 – Secure Data Exchange

8.5.2.2 Secure Data message

8.5.2.2.1 Structure

Each Secure Data message shall contain the information described in 8.5.2.1 and summarized in Table 28.

In the Secure Data message, the station shall include the ASDU to be transmitted described in 8.5.2.2.6.

Table 29 – Secure Data message

Value Value	AIM = Controlling station association ID
Value Value	AIS = Controlled station association ID
Value Value Value Value	DSQ = Data Sequence Number
Value Value	ADL = Application Data Length
Data structure containing authenticated application data, depending by the algorithm used	SDP = Secure Data Payload

8.5.2.2.2 Controlling station Association ID

This is the value the controlling station has chosen to represent the communication link with this controlled station. This value shall match the AIM in the last Update Key Change Request sent to the controlled station during the successful Station Association procedure most recently performed for this communication link, described in 8.3.5.4.

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

8.5.2.2.3 Controlled station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. This value shall match the AIS in the last Update Key Change Response received from the controlled station during the successful Station Association procedure most recently performed for this communication link, described in 8.3.5.5.

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

8.5.2.2.4 Data Sequence Number

Each station shall maintain a Data Sequence Number according to the following rules.

a) The device shall use a separate DSQ in each direction, for each Association ID.

b) The DSQ value in the first Secure Data message transmitted by either device after successful Session Key initialization must be 1 (i.e. after the controlled station received an authentic Session Key Change Request or the controlling station received an authentic Session Key Change Response)

c) The DSQ shall be incremented by one in each new Secure Data message transmitted.

d) The receiver of a Secure Data message shall discard the message if the DSQ *is less* than the next expected value. The expected value shall be:

   – the value in the last Secure Data message in that direction plus one or

   – 1 (one) immediately after a successfully executed Session Key Change procedure.

e) The receiver of a Secure Data message shall consider the DSQ value received only if the message is correctly authenticated.

f) The DSQ shall never be zero, the controlling station shall re-initialize the session keys before the DSQ would roll over from 4294967295 to 0.

DSQ:= UI32[1..32]<1.. 4294967295>

8.5.2.2.5 Application Data Length

This value shall specify the length in octets of the entire Application Service Data Unit (ASDU) to be authenticated and transmitted, contained in the Secure Data Payload that follows.

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

8.5.2.2.6 Secure Data Payload

8.5.2.2.6.1 General

Data structure containing the ASDU to be transmitted and authentication information. The structure of the Secure Data Payload is determined by the Data Protection Algorithm (DPA) selected by the controlling station in the successful Session Key Change procedure most recently executed, described in 8.4.

8.5.2.2.6.2 Secure Data Payload using MAC algorithm

If a MAC algorithm is selected to authenticate application data, the structure of the Secure Data Payload is illustrated in Table 30.

Table 30 – Secure Data Payload using MAC algorithm

Defined by the referencing standard Number of octets specified in ADL	ASDU = Application Service Data Unit
Number of octets specified by the MAC algorithm selected in DPA during the last Session Key Change procedure	MAC = Message Authentication Code

The Application Service Data Unit is the entire ASDU to be authenticated and transmitted, not including data link layer or APCI information.

ASDU:= OS8i[1..8i]; i:=ADL

The Controlling station shall use the current Control Direction Session Key to calculate the MAC value in the messages to be transmitted, and the current Monitor Direction Session Key to verify the MAC value in the messages received.

The Controlled station shall use the current Monitoring Direction Session Key to calculate the MAC value in the messages to be transmitted, and the and the current Control Direction Session Key to verify the MAC value in the messages received

Each station shall pass the data through the MAC Algorithm in the order described in Table 31, referencing standards may require further information, in addition to those indicated in

Table 31, to be included in the MAC calculation, The length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in 8.4.2.4.4.

Table 31 – Data included in the MAC calculation in Secure Data Payload (in order)

Data	Description	Described in	Source
Secure Data message values	The entire Secure Data message being transmitted up to and including the ASDU in the Secure Data Payload (excluding the MAC field).	Subclause 8.5.2.2	Secure Data Message
Padding Data	As required by the MAC algorithm.	Algorithm specification	Required by algorithm.

MAC:= OS8i[1..8i]; i:=as specified in the MAC algorithm selected (DPA) in the last authentic Session Key Change Request transmitted by the controlling station, defined in 8.4.2.3.4.

8.5.2.2.6.3 Secure Data Payload using AEAD algorithm

If AEAD algorithm is used to encrypt and authenticate application data, the Secure Data Payload is entirely provided as output by the AEAD algorithm.

The Controlling stations shall use the current Control Direction Session Key as the secret key K in the AEAD algorithm to encrypt the application data in the messages to be transmitted, and the current Monitoring Direction Session Key as the secret key K in the AEAD algorithm to decrypt the application data in the messages received.

The Controlling stations shall use the current Monitoring Direction Session Key as the secret key K in the AEAD algorithm to encrypt and authenticate application data in the messages to be transmitted, and the current Control Direction Session Key as the secret key K in the AEAD algorithm to decrypt and verify the application data in the messages received.

Table 32 describes the parameters to be provided to the AEAD algorithm, in the order listed, to obtain the Secure Data Payload in this message. Referencing standards may require further information, in addition to those indicated in Table 32, to be included in the parameters of the AEAD algorithm.

Table 32 – AEAD algorithm parameters to generate the Secure Data Payload (in order)

Data	Description	Described in	AEAD algorithm parameter
Controlling station Association ID and Controlled station Association ID	The AIM and AIS values concatenated in this order to obtain a 32bit value.	Subclauses 8.5.2.2.2 and 8.5.2.2.3	Used as Additional Data in the algorithm (A)
Data Sequence Number	The DSQ value in this message	Subclause 8.5.2.2.4	Padded with zeroes to obtain 12 octets, used as Nonce (N)
Application Data Length	The ADL value in this message	Subclause 8.5.2.2.5	Concatenated in this order and used as data to be encrypted or decrypted (P)
Application Service Data Unit	The entire ASDU to be transmitted, not including data link layer or APCI information.	Protocol specification	

Note that the Application Data Length (ADL) in this message is used as a secondary check of the validity of the data after decryption.

8.5.3 Controlling station state machine

On the controlling station, the Secure Data Exchange messages described in 8.5.2 shall be managed by the state machine described in 8.5.3. Figure 12 illustrates an overview (informative) of the v Secure Data Exchange transactions on controlling station. The controlling station shall execute the Secure Data Exchange state machine described in Table 32 (normative).

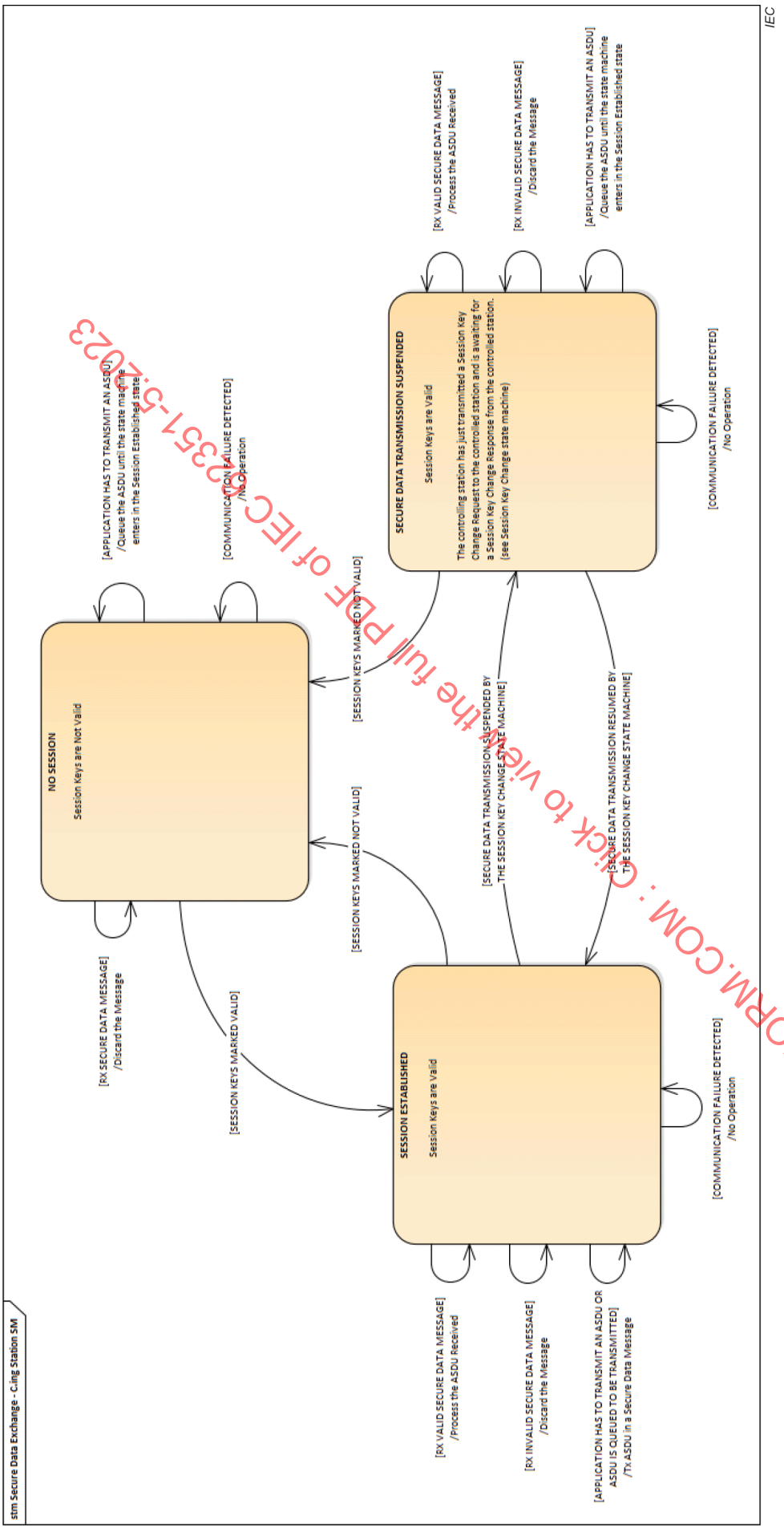


Figure 12 – Secure Data Exchange – Controlling station state machine

Table 33 – Controlling station state machine: Secure Data Exchange

Event	Event Description	State						
		No Session		Session Established		Secure Data Transmission Suspended		
		Session Keys are Not Valid		Session Keys are Valid		Secure data transmission suspended by the Session Key Change state machine		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Rx valid Secure Data message	The controlling station receives a valid Secure Data message.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Increment the *Successful Data Authentications* statistic Process the Secure Data message ASDU	Session Established	Increment the *Successful Data Authentications* statistic Process the Secure Data message ASDU	Secure Data Transmission Suspended	1
Rx Invalid Secure Data message: the message is not authentic	The controlling station receives a Secure Data message with invalid authentication information	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Increment the *Data Authentication Errors* statistic. Discard the message Increment *Discarded Messages* statistic.	Session Established	Increment the *Data Authentication Errors* statistic. Discard the message Increment *Discarded Messages* statistic.	Secure Data Transmission Suspended	2
Rx Invalid Secure Data message: the message contains parameter error(s).	The controlling station receives a correctly authenticated Secure Data message, with one of the following error conditions: The controlling station Association ID is incorrect. The controlled station Association ID is incorrect. The DSQ is lower than the expected value	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Established	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Secure Data Transmission Suspended	3

Event	Event Description	State						
		No Session		Session Established		Secure Data Transmission Suspended		
		Session Keys are Not Valid		Session Keys are Valid		Secure data transmission suspended by the Session Key Change state machine		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
The controlling station has to Transmit an ASDU	A user (or application) wishes to transmit an ASDU or an ASDU is pending (queued) to be transmitted.	Queue the ASDU until the next time the controlling station enters in the "*Session Established*" state	No Session	Transmit the ASDU by sending the Secure Data message.	Session Established	Queue the ASDU until the next time the controlling station enters in the "*Session Established*" state	Secure Data Transmission Suspended	4
Secure Data Transmission suspended by the Session Key Change state machine	The controlling station has just transmitted a Session key Change Request message and is waiting for a Session Key Change Response from the controlled station	No Operation	No Session	No further operation is required other than changing to the "*Secure Data Transmission Suspended*" state.	Secure Data Transmission Suspended	No Operation. (This event should occur only when the state machine is in the "*Session Established*" state)	Secure Data Transmission Suspended	5
Secure Data Transmission resumed by the Session Key Change state machine	The controlling station has completed the Session Key Change procedure.	No Operation	No Session	No Operation. (This event should occur only when the state machine is in the "*Secure Data Transmission Suspended*" state)	Session Established	No further operation is required other than changing to the "*Session Established*" state.	Session Established	6
Communication Failure Detected Note: this event shall be considered if communication failures can be detected in the communication link	The controlling station has detected a communication failure.	No Operation.	No Session	No Operation.	Session Established	No Operation.	Secure Data Transmission Suspended	7

Event	Event Description	State						
		No Session		Session Established		Secure Data Transmission Suspended		
		Session Keys are Not Valid		Session Keys are Valid		Secure data transmission suspended by the Session Key Change state machine		
		Action	Next State	Action	Next State	Action	Next State	
A	B	C	D	E	F	G	H	
Session Keys marked Valid.	The Session Keys were marked Valid by the Session Key Change state machine.	No further operation is required other than changing to the “Session Established” state.	Session Established	Discard the event. (This event can occur only when the state machine is in the “No Session” state)	Session Established	Discard the event. (This event can occur only when the state machine is in the “No Session” state)	Secure Data Transmission Suspended	8
Session Keys marked Not Valid.	The Session Keys were marked Not Valid by the Session Key Change state machine.	Discard the event. (This event can occur only when the state machine is in the “Session Established” state or in the “Secure Data Transmission Suspended” state)	No Session	No further operation is required other than changing to the “No Session” state.	No Session	No further operation is required other than changing to the “No Session” state.	No Session	9

8.5.4 Controlled station state machine

On the controlled station, the Secure Data messages described in 8.5.2 shall be managed by the state machine described in 8.5.4. Figure 13 illustrates an overview (informative) of the Security Normal Operations transactions on controlled station. The controlled station shall execute the Security Normal Operations state machine described in Table 34 (normative).

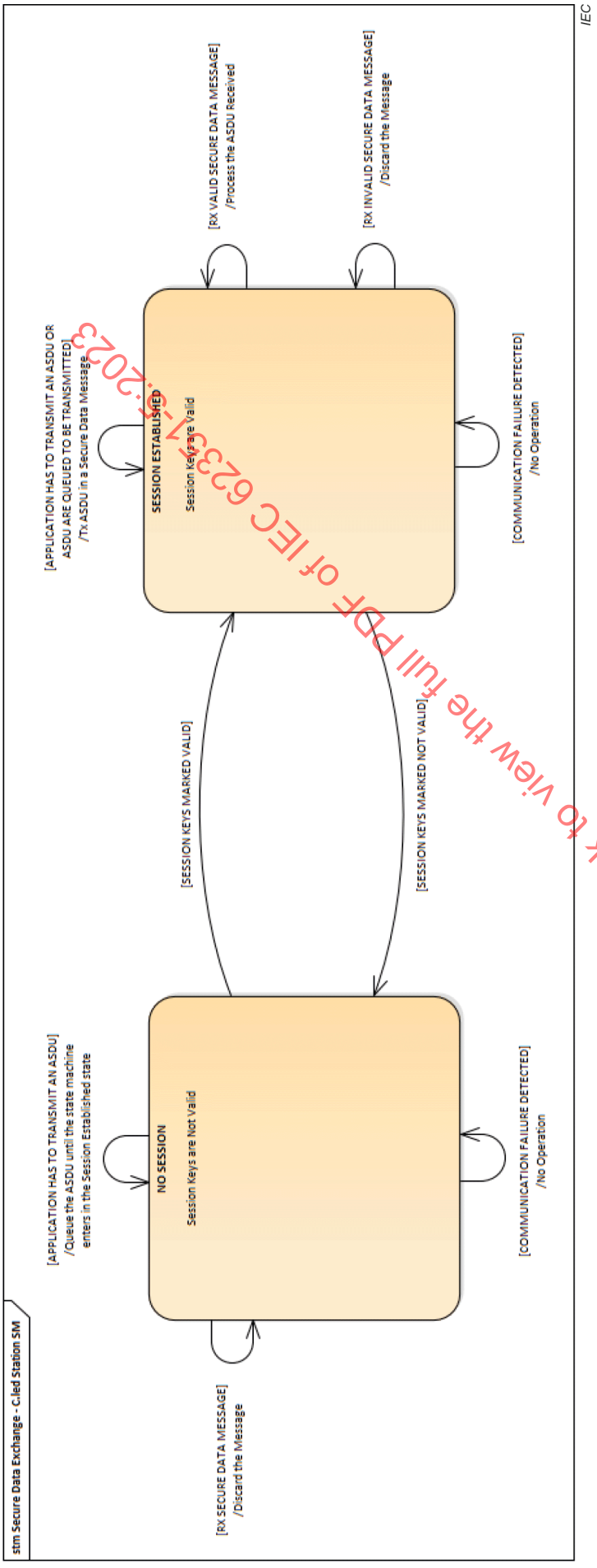


Figure 13 – Secure Data Exchange – Controlled station state machine

Table 34 – Controlled station state machine: Secure Data Exchange

Event	Event Description	State				
		No Session		Session Established		
		Session Keys are Not Valid		Session Keys are Valid		
		Action	Next State	Action	Next State	
A	B	C	D	G	H	
Rx Valid Secure Data message.	The controlled station receives a correctly authenticated Secure Data message with valid parameters	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Process the Secure Data message ASDU. Increment the *Successful Data Authentications* statistic	Session Established	1
Rx Invalid Secure Data message: the message is not authentic	The controlling station receives a Secure Data message with invalid authentication information.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Increment the *Data Authentication Errors* statistic. Discard the message Increment the *Discarded Messages* statistic.	Session Established	2
Rx Invalid Secure Data message: the message contains parameter error(s).	The controlling station receives a correctly authenticated Secure Data message with one of the following error conditions: a) The controlling station Association ID is incorrect. b) The controlled station Association ID is incorrect. c) The DSQ is lower than the expected value	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	No Session	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic.	Session Established	3

Event	Event Description	State				
		No Session		Session Established		
		Session Keys are Not Valid		Session Keys are Valid		
		Action	Next State	Action	Next State	
A	B	C	D	G	H	
Rx Invalid Secure Data message: The requested operation is not permitted.	The controlled station receives a correctly authenticated Secure Data message requesting an operation not authorized to the role assigned to the controlling station.	Increment the *Unexpected Messages* statistic. Discard the message. Increment the *Discarded Messages* statistic	No Session	Increment the *Operation Authorization Failures* statistic. Discard the message Increment the *Discarded Messages* statistic	Session Established	4
The controlled station has to Transmit an ASDU	An application wishes to transmit an ASDU from this controlled station.	Queue the ASDU until the controlling station enters in the *Session Established* state (when Session Keys are marked Valid by the Session Key change state machine).	No Session	Transmit the ASDU by sending the Secure Data message.	Session Established	5
Communication Failure Detected Note: this event shall be considered if communication failures can be detected in the communication link	The controlled station has detected a communication failure	No Operations.	No Session	No Operations.	Session Established	6
Session Keys Marked Valid.	The Session Keys were marked Valid by the Session Key Change state machine.	No further operation is required other than changing to the “Session Established” state.	Session Established	Discard the event. (This event can occur only when the state machine is in the “No Session” state)	Session Established	7
Session Keys Marked Not Valid.	The Session Keys were marked Not Valid by the Session Key Change state machine.	Discard the event. (This event can occur only when the state machine is in the “Session Established” state)	No Session	No further operation is required other than changing to the “No Session” state.	No Session	8

8.5.5 Controlling station directives for Secure Data Exchange

8.5.5.1 General

The controlling station shall increment the Session Key Usage Counter each time a Secure Data message is transmitted and each time a valid Secure Data message is received.

Additionally, the controlling station shall be able to transmit and receive Secure Data messages while executing the Station Association and Session Key Change procedures as described respectively in 8.5.5.1 and 8.5.5.2.

8.5.5.2 Secure Data Exchange during Station Association

The controlling station shall be able to send Secure Data messages pending to be transmitted as well as accept and process the Secure Data message received during the Station Association procedure if the Session Key are valid. In particular:

– Awaiting the Association Response from the controlled station (i.e. the state machine is in "Wait for Association Response" status described in Table 15) after sending an Association Request to the controlled station.

– Awaiting the Update Key Change Response from the controlled station (i.e. the state machine is in "Wait for Update Key Change Response" status described in Table 15) after sending an Update Key Change Request to the controlled station.

8.5.5.3 Secure Data Exchange during Session Key Change

The controlling station shall always accept and process the Secure Data message received during the Session Key Change procedure if the Session Key are valid. In particular:

– Awaiting the Session Response from the controlled station (i.e. the state machine is in "Wait for Session Response" status described in Table 26) after sending a Session Request to the controlled station.

– Awaiting the Session Key Change Response from the controlled station (i.e. the state machine is in "Wait for Session Key Change Response" status described in Table 26) after sending a Session Key Change Request to the controlled station.

The controlling station shall be able to send Secure Data message pending to be transmitted while executing the Session Key Change procedure if the Session Keys are valid and in the following conditions:

– Awaiting the Session Response from the controlled station (i.e. the state machine is in "Wait for Session Response" status described in Table 26) after sending a Session Request to the controlled station.

The controlling station shall not send Secure Data message pending to be transmitted during the Session Key Change phase, even if the Session Keys are valid, in the following conditions:

– Awaiting the Session Key Change Response from the controlled station (i.e. the state machine is in "Wait for Session Key Change Response" status described in Table 26) after sending a Session Key Change Request to the controlled station.

8.5.6 Controlled station directives for Secure Data Exchange

8.5.6.1 General

The controlled station shall increment the Session Key Usage Counter each time a Secure Data message is transmitted and each time a valid Secure Data message is received.

The controlled station shall be able to send Secure Data messages pending to be transmitted and process the Secure Data message received at any time if the Session Keys are valid. Priority must be given at the responses to the controlling station requests.

8.5.6.2 Enforcing controlling station roles

If the Role Base Access control is supported, the controlled station shall enforce the Roles assigned to the controlling station, as described in 8.3.12.2, retrieved during the Station Association procedure, described in 8.3. The controlled station shall not permit the controlling station to perform actions it does not have permission to perform, as designated by its Role, regardless of whether the controlling station's certificate is authentic (the Station Association procedure was successfully performed).

In case the controlling station requests an operation not authorized to perform, the controlled station shall respond with a negative response using the affected protocol. The affected protocol referencing standards shall specify how the controlled station shall respond by the affected protocol.

8.5.7 Example of Secure Data exchange during Station Association

Figure 14 illustrates how Secure Data messages are exchanged while the stations are executing the Station Association procedure and the current Session Keys are valid.

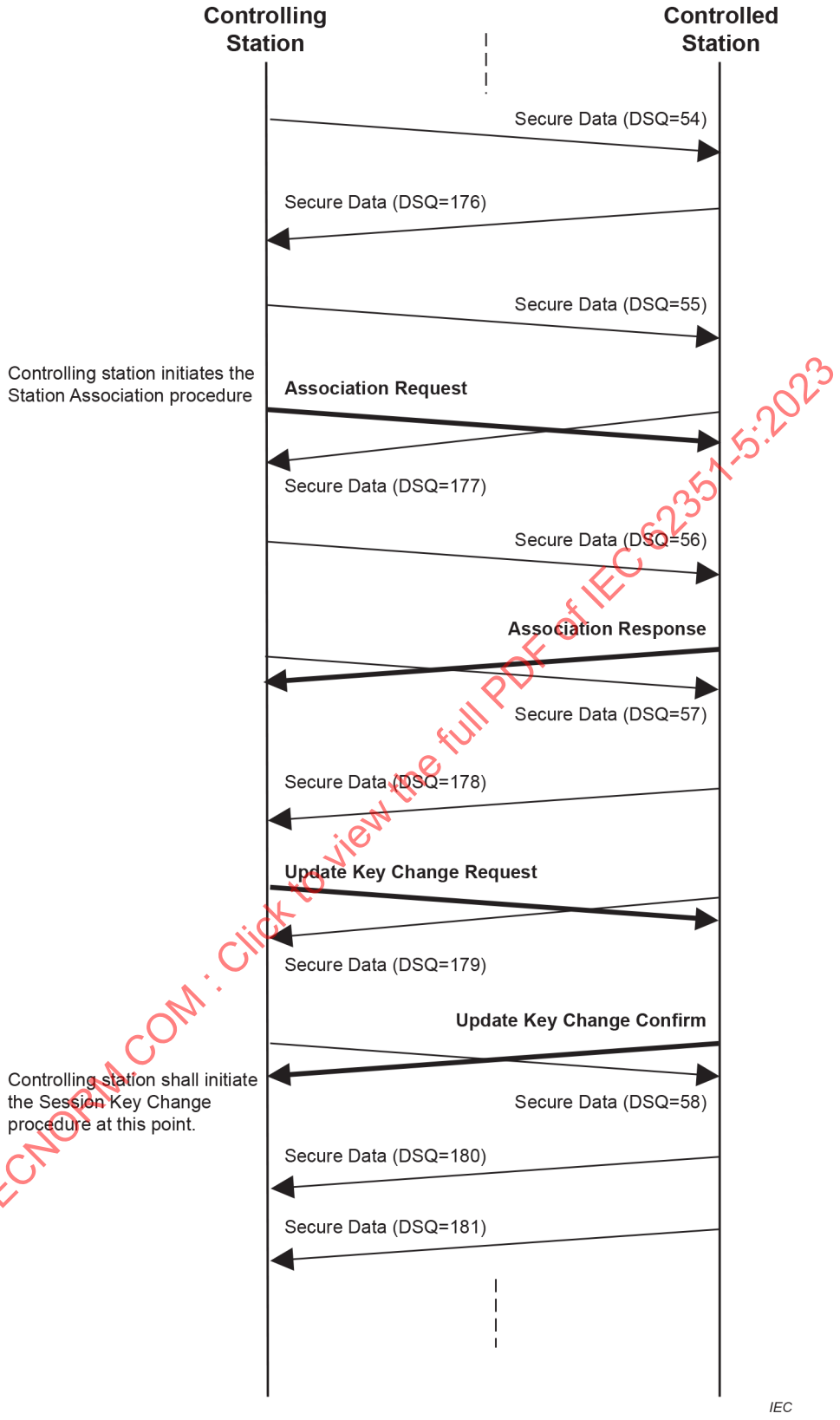


Figure 14 – Example of Secure Data Exchange during Station Association

8.5.8 Example of Secure Data Exchange during Session Key Change

Figure 15 illustrates how Secure Data messages are exchanged while the stations are executing the Session Key Change procedure and the current Session Keys are still valid.

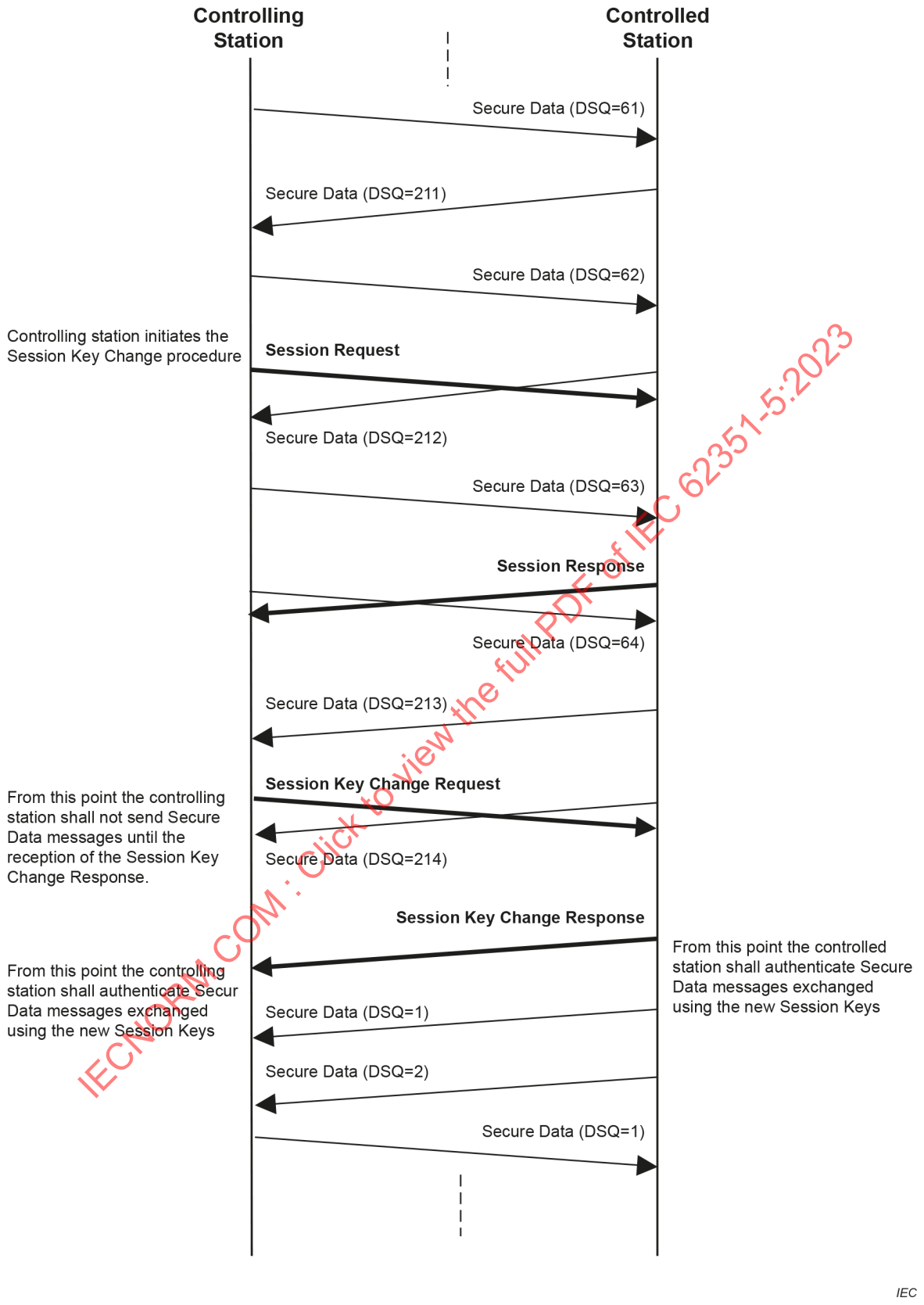


Figure 15 – Example of Secure Data messages exchanged during Session Key Change

9 Interoperability requirements

9.1 Overview of clause

Clause 9 describes which capabilities shall be considered to fall into the following categories:

– mandatory to ensure interoperability between stations;
– optional but required to be tested if implemented.

9.2 Minimum requirements

9.2.1 Overview of subclause

Subclause 9.2 describes the mandatory minimum capabilities required for a station to comply with this document.

9.2.2 Authentication algorithms

9.2.2.1 Requirements on each station

Each station shall implement the authentication algorithms listed in 9.2.2.

9.2.2.2 HMAC-SHA-256

Each station shall permit the use of HMAC-SHA-256, as described in RFC 2104, to calculate the HMAC Value. The HMAC Value shall be the 256 bits (32 octets) output of the HMAC algorithm, truncated to either the leftmost 8 octets or the leftmost 16 octets. If this specification is used over TCP/IP, the truncated value shall be 16 octets. If it is used over serial links, the truncated value shall be 8 octets.

This shall be the default authentication algorithm.

9.2.2.3 ECDSA-with-SHA256

Each station shall permit the use of the Elliptic Curve Digital Signature Algorithm (ECDSA), defined in ANSI X9.62, using the SHA-256 secure hash algorithm.

9.2.2.4 RSA-2048-with-SHA256

Each station shall permit the use of the RSA signature algorithm, defined in ANSI X9.31, using the SHA-256 secure hash algorithm.

9.2.3 Key wrap / transport algorithms

9.2.3.1 Requirements on each station

Each station shall implement key wrap or key transport algorithms as described in 9.2.3.

9.2.3.2 AES-256 Key Wrap

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

This shall be the default Key Wrap algorithm.

9.2.4 Cryptographic keys

9.2.4.1 Requirements on each station

Each station shall support the cryptographic keys as described in 9.2.4.

9.2.4.2 Minimum Session Keys size

The minimum size of the Session Keys used to authenticate application data shall be 256 bits.

9.2.4.3 Minimum Update Keys size

The minimum size of the Encryption Update Keys (used to wrap and unwrap Session Keys) and the Authentication Update Key (used to authenticate the Station Association and Session Key Change procedures) shall be 256 bits.

9.2.4.4 Minimum public key size

The minimum size of the device's public key used to derive the Update Keys shall be 256 bits. The utilized public key is an ECDH key according to subclause 8.3.2.

9.2.5 Cryptographic curves

9.2.5.1 Requirements on each station

Each station shall support the following EC curves:

– Curve 25519
– Curve 448
– secp256k1
– secp256r1

9.2.6 Configurable values

9.2.6.1 Requirements on each station

Each station shall permit a human to change the parameters described in 9.2.6. Changes to these parameters shall be permanently retained over restarts of the station. The affected protocol referencing standards shall specify the default value and the maximum value of these parameters.

9.2.6.2 Remote station's public key or certificate fingerprint.

Both controlling and controlled stations use this parameter during the Station Association procedure, described in 8.3, to verify the remote station's certificate if self-signed device certificates are used.

9.2.6.3 Expected Reply Time

The Expected Reply Time is used by the controlling station to detect communication failures. This parameter shall be configurable in seconds. The default value shall be 2 sec. The maximum configurable value shall be at least 120 s.

9.2.6.4 Expected Request Time

The Expected Request Time is used by the controlled station to detect communication failures. This parameter shall be configurable in seconds. This value should be the value of Expected Reply Time multiplied by Max Reply Timeouts (both configured in the controlling station as described respectively in 9.2.6.3 and 9.2.6.8).

9.2.6.5 Max Session Key Usage Time

Both controlling and controlled stations use this parameter to determine the Session Key change time interval. This parameter shall be configurable in minutes. The default value shall be 15 min.

To accommodate systems which communicate infrequently (for instance every few hours or days), it shall be possible to disable the Session Key Usage Timer and use only the Session Key Usage Count. Alternately, the station may permit Session Key Usage Time up to 1 week in length.

To avoid the controlled station to invalidate the current Session Keys before that the controlling station changes the Session Keys, it is recommended that the controlled station interval be configured for twice the interval configured at the controlling station.

9.2.6.6 Max Session Key Usage Count

The controlling station shall also change Session Keys whenever a configured number of Secure Data messages has been transmitted in either direction since the last successfully performed Session Key Change procedure. The value shall be configurable from one in increments of one. The default value shall be 1 000. The maximum configurable value shall be 65534.

To avoid the controlled station to invalidate the current Session Keys before that the controlling station changes the Session Keys, it is recommended that the controlled station count be configured for twice the count configured at the controlling station.

9.2.6.7 Security statistic thresholds

The controlled station shall permit an event threshold to be configured for each of the security statistics listed in Table 7. If the statistic has incremented by the amount of the threshold since either startup or since the last time the statistic was reported, the controlled station shall report the statistic to the controlling station by the affected protocol.

9.2.6.8 Special security thresholds

The controlling station shall permit the Max Reply Timeouts threshold value to be configured.

9.2.6.9 Authorized remote stations

Each station (controlling and controlled) shall permit to configure the list with the public keys of the remote station authorized to communicate with the local station. The public keys in this list shall match the public key in the certificates of the authorized remote stations.

If the Central Authority is supported, each station (controlling and controlled) shall permit to configure the list with the Distinguished Names of the remote stations authorized to communicate with the local station. The Distinguished Names in this list shall match the distinguished name in the certificates of the authorized remote stations. The Organization's security policy may require to use this feature to increase security.

9.2.6.10 Disabling secure communication

Each station shall permit this secure communication mechanism to be completely disabled by configuration on a per-remote station basis: a controlling station shall be able to disable secure communication to any controlled station and a controlled station shall be able to disable secure communication to any controlling station.

The default shall be that secure communication is enabled.

9.2.7 Cryptographic information

Table 34 contains the list of the cryptographic information and the correspondence between these pieces of information, mandatory and optional to be retained by devices over restarts. Table 35 contains the legend of the operations listed in Table 34.

Table 35 – Configuration of cryptographic information

Information	Central Authority	Controlling station	Controlled station	To be retained over restarts (m=mandatory, o=optional)
Monitoring Direction Session Key	-	Derive	Rx	o
Control Direction Session Key	-	Derive	Rx	o
Encryption Update Key	-	Derive	Derive	m
Authentication Update Key	-	Derive	Derive	m
Local Station Name	Config	Config	Config	m
Remote Station Name	Config	Config	Config	m
Central Authority Private Key	Derive	-	-	m
Central Authority Public Key	Derive	Config	Config	m
Local Station Private Key	-	Derive	Derive	m
Local Station Public Key	Sign (if CA is supported).	Derive	Derive	m
Remote Station Certificate Data	Sign (if CA is supported)	Rx	Rx	m
Remote Station Public Key or Certificate Fingerprint		Config	Config	m

Table 36 – Legend for configuration of cryptographic information

Cell text	Meaning
Derive	This entity shall derive (create) the information
Sign	This entity shall sign (authenticate) the information
Rx	This entity shall receive the information via data communications
Config	This entity shall have this information pre-configured
-	This entity does not use the information

9.3 Options

9.3.1 Overview of subclause

Subclause 9.3 describes capabilities in compliance with this specification, that may be implemented as options. If a station implements these capabilities, they shall be verified for compliance. If a station implements any capabilities not listed in 9.3, the station must provide a mode in which these capabilities are disabled.

9.3.2 MAC/AEAD algorithms

9.3.2.1 General

Each station may implement additional MAC/AEAD algorithms in addition to those listed as mandatory. A station may be configured to reject particular mandatory MAC/AEAD algorithms, but it shall be able to support all the mandatory MAC/AEAD algorithms.

9.3.2.2 HMAC-SHA3-256

Each station may implement HMAC-SHA3-256 algorithm, as described in NIST FIPS 202 to calculate the MAC Value. The MAC value shall be the 256 bits (32 octets) output of the HMAC algorithm, truncated to either the leftmost 8 octets or the leftmost 16 octets. If this specification is used over TCP/IP, the truncated value shall be 16 octets. If it is used over serial links, the truncated value shall be 8 octets.

9.3.2.3 BLAKE2s-256

Each station may implement BLAKE2s-256 algorithm, as described in RFC 7693 to calculate the MAC Value. The MAC value shall be the 256 bits (32 octets) output of the BLAKE2s algorithm, truncated to either the leftmost 8 octets or the leftmost 16 octets. If this specification is used over TCP/IP, the truncated value shall be 16 octets. If it is used over serial links, the truncated value shall be 8 octets.

9.3.2.4 AEAD-AES-256-GCM

Each station may implement AEAD-AES-256-GCM algorithm, as described in RFC 5116, to encrypt/decrypt and authenticate data at the same time.

9.3.3 Key wrap / transport algorithms

Each station may implement additional Key Wrap algorithms in addition to those listed as mandatory. The controlled station may be configured to reject particular mandatory key wrap algorithms, but it shall be able to support all the mandatory key wrap algorithms.

9.3.4 Cryptographic curves

Each station may support the following EC curves:

– brainpoolP256r1

9.4 Use with TCP/IP

Protocols that implement IEC 62351-5 over profiles including TCP/IP and require confidentiality should use transport security (T-Profile) in compliance with IEC 62351-3. The affected protocol referencing standards shall meet the requirements for referencing that standard.

The relationship between TCP connection management and this document shall be discussed in the individual affected protocol referencing standards.

Use of IEC 62351-5 with other IP networking security mechanisms (e.g. IPSec) is out of the scope of this specification.

9.5 Use with redundant channels

When used with redundant channels, if primary and redundant channel share all the security mechanism information, the communication link shall not be considered to have failed until all channels have been tried.

10 Requirements for referencing this standard

10.1 Overview of clause

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

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

Clause 10 describes the information that shall be included in any protocol specification that references this specification.

10.2 Selected options

The affected protocol referencing standards shall identify which of the options identified in 9.3 are mandatory for the protocol (if any).

The affected protocol referencing standards shall identify any additional security algorithms, fixed parameters, configurable parameters or features supported by the protocol beyond the mandatory set specified in 9.2.

10.3 Message format mapping

The affected protocol referencing standards shall describe how each of the messages described in Clause 8 shall be implemented using the affected protocol.

The message formats described in the affected protocol referencing standards shall include all information found in the messages described in this document.

In general, the affected protocol referencing standards shall use the sequence, layout, and naming of information described in this document.

The affected protocol referencing standards shall not reduce the size or range of any information described in this document.

10.4 Reference to procedures

The affected protocol referencing standards shall specify how the procedures described in Clause 8 shall be implemented using the affected protocol.

If there is a disagreement between the procedures described in the affected protocol referencing standards and the procedures described in this document, this document shall be deemed to be the correct description.

10.5 Protocol information

The affected protocol referencing standards shall specify the data structure and possible values of the protocol information and the protocol version in the Protocol Information field provided by the controlling station in the Station Association and in the Session Key Change procedures described in Clause 8.

The affected protocol referencing standards shall also specify how the controlled station shall manage and validate the Protocol Information value and different protocol versions in this field.

10.6 Controlled station response to unauthorized operations requests

The affected protocol referencing standards shall specify how the controlled station shall respond to the controlling station by the affected protocol in case the controlling station requests an operation not authorized to perform (see "Enforcing controlling station role", 8.5.6.2).

10.7 Transmission of security statistics

The affected protocol referencing standards shall specify the method to transmit security statistics counters from the controlled station by the affected protocol.

10.8 Configurable values

The affected protocol referencing standards shall specify the default value and the maximum value of configurable values described in 9.2.6.

10.9 Protocol implementation conformance statement

The affected protocol referencing standards shall provide the PICS section used by the implementors to supply information about the features supported by the device.

The PICS section must contain all the mandatory and optional features described in Clause 9 in conjunction with the additional mandatory and optional features defined in the affected protocol referencing standards.

Annex A
(informative)

Security Event mapping to IEC 62351-14

A.1 General

This annex contains the mapping of the security events defined in this document to the format specified in IEC 62351-14.

The information about the security events and potential detailed information to be contained in the ExtraInfo may only be provided by the entity based on the availability of this information through the underlying platform or utilized components.

A.2 Mapping of IEC 62351-5 events specified in this document

The IEC Version of all security events shall be “1”.

For the security events identifier, the following grouping is used:

– Value “1” relates to the secure communication procedures
– Value “2” relates to the certificate verifications

Table A.1 – Security event logs defined in IEC 62351-5 Ed.1 mapped to IEC 62351-14

Security Event	MNEMONIC	Severity	Event identifier	Text
The Station Association procedure was successfully performed	STAS_PROC_SUCC.	notice	62351-5:1.1	Station Association successfully performed
The Station Association procedure has failed	STAS_PROC_FAIL	alarm	62351-5:1.2	Station Association Failed
The Session Key Change procedure was successfully performed.	SKEY_PROC_SUCC	notice	62351-5:1.3	Session Key Change successfully performed.
The Session Key Change procedure has failed.	SKEY_PROC_FAIL	alarm	62351-5:1.4	Session Key Change failed
The Session Keys were invalidated because the Max Session Key Usage Time expired	SKEY_INV_USETOUT	alarm	62351-5:1.5	Session Key invalidated due to Max Session Key Usage Timeout
The Session Keys were invalidated because the Max Session Key Usage Count has exceeded.	SKEY_INV_USECNT	alarm	62351-5:1.6	Session Key invalidated due to Max Session Key Usage Count
The controlling station provided invalid protocol information	PROT_INFO_ERR	alarm	62351-5:1.7	Invalid protocol Information
The Key Authentication Algorithm is not supported.	KEY_AUTNALG_SUP	alarm	62351-5:1.8	Key authentication algorithm not supported
The Key Wrap Algorithm is not supported.	KEY_ WRAPALG _SUP	alarm	62351-5:1.9	Key wrap algorithm not supported
Data Protection Algorithm not supported	DATA_PROTALG_SUP	alarm	62351-5:1.10	Data protection algorithm not supported
Key Authentication Error	KEY_AUTN_ERR	alarm	62351-5:1.11	Session Key authentication error

Security Event	MNEMONIC	Severity	Event identifier	Text
Data Authentication Error	DATA_AUTN_ERR	warning	62351-5:1.12	Data authentication error
Unexpected Message	UNXP_MSG_ERR	warning	62351-5:1.13	Unexpected message error
Max Reply Timeouts	MAX_REPLY_TOUT	warning	62351-5:1.14	Max reply timeouts reached
The remote station is not authorized to communicate.	NODE_NOT_AUTR.	alarm	62351-5:2.1	Remote station not authorized
The controlling station is not authorized to perform the requested operation	OPER_NOT_AUTR	warning	62351-5:2.2	Requested operation not authorized
Remote Station's Certificate Check Failed.	REM_CERT_NOTVALID	alarm	62351-5:2.3	Invalid remote station's certificate
The remote station's certificate Expired.	REM_CERT_EXPIRED	warning	62351-5:2.4	Remote station's certificate expired.
The remote station's certificate has been revoked.	REM_CERT_REVOKED	alarm	62351-5:2.5	Remote station's certificate revoked.
The local station's certificate Expired.	LOC_CERT_EXPIRED	warning	62351-5:2.6	Local station's certificate expired.
The local station's certificate has been revoked.	LOC_CERT_REVOKED	alarm	62351-5:2.7	Local station's certificate revoked.
Cryptographic Keys invalidated because the remote station's certificate has been revoked.	KEYS_INV_REMCERTREV	alarm	62351-5:2.8	Cryptographic Keys invalidated due to remote station certificate revocation.
Cryptographic Keys invalidated because the local station's certificate has been revoked.	KEYS_INV_LOCCERTREV	alarm	62351-5:2.9	Cryptographic Keys invalidated due to local station certificate revocation.

Bibliography

IEC TR 60870-1-3, *Telecontrol equipment and systems – Part 1: General considerations – Section 3: Glossary*

IEC 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

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

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

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

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

IEEE 1815-2012, *Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)*

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

IETF RFC 4086, Randomness Requirements for Security

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information*

IETF RFC 5639, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*

IETF RFC 5758, *Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA*

IETF RFC 8017, *PKCS #1: RSA Cryptography Specifications Version 2.2*

NIST FIPS 180-4, *Secure Hash Standard (SHS)*

NIST FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*

NIST IR 7298, *Glossary of Key Information Security Terms*

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

NIST SP 800-90A Rev.1, *Recommendation for Random Number Generation Using Deterministic RBGs*

NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation.

NIST SP 800-90C Rev.1, Recommendation for Random Bit Generator (RGB) Construction.

SOMMAIRE

AVANT-PROPOS 128
1 Domaine d'application 130
2 Références normatives 131
3 Termes et définitions 132
4 Abréviations 133
5 Description de problème 134
5.1 Vue d'ensemble de l'article 134
5.2 Menaces spécifiques traitées 134
5.3 Problèmes de conception 134
5.3.1 Vue d'ensemble du paragraphe 134
5.3.2 Communications asymétriques 134
5.3.3 Orientés message 135
5.3.4 Numéros de séquence faibles ou absence de numéros de séquence 135
5.3.5 Puissance de traitement limitée 135
5.3.6 Largeur de bande limitée 135
5.3.7 Pas d'accès au serveur d'authentification 136
5.3.8 Longueur de trame limitée 136
5.3.9 Somme de contrôle limitée 136
5.3.10 Systèmes radio 136
5.3.11 Systèmes commutés 136
5.3.12 Diversité des protocoles concernés 137
5.3.13 Couches liaison de données différentes 137
5.3.14 Intervalles d'amélioration longs 137
5.3.15 Sites à distance 137
5.3.16 Supports peu fiables 137
5.4 Principes généraux 137
5.4.1 Vue d'ensemble du paragraphe 137
5.4.2 Couche application seulement 138
5.4.3 Définition générique mise en correspondance avec différents protocoles 138
5.4.4 Bidirectionnel 138
5.4.5 Gestion des clés cryptographiques 138
5.4.6 Rétrotolérance 138
5.4.7 Possibilité de mise à jour 138
5.4.8 Connexions multiples 139
6 Théorie de fonctionnement 139
6.1 Vue d'ensemble de l'article 139
6.2 Communication sécurisée 139
6.2.1 Concepts fondamentaux 139
6.2.2 ID d'Association 140
6.2.3 Authentification 140
6.2.4 Autorité Centrale 141
6.2.5 Contrôle d'Accès Basé sur les Rôles (RBAC) 141
6.2.6 Clés cryptographiques 141
6.2.7 Statistiques de sécurité 145
6.2.8 Événements de sécurité 145
7 Exigences fonctionnelles 145

7.1 Vue d'ensemble de l'article 145
7.2 Vue d'ensemble des procédures 145
7.3 Vue d'ensemble des diagrammes d'états 146
7.4 Horloges et compteurs 148
7.5 Statistiques de sécurité et événements 149
7.5.1 Généralités 149
7.5.2 Seuils de sécurité spéciaux 153
7.5.3 Rapport des statistiques de sécurité 153
7.5.4 Surveillance et enregistrement des événements de sécurité 154
8 Procédures formelles 154
8.1 Vue d'ensemble du paragraphe 154
8.2 Distinction entre messages et ASDU 154
8.2.1 Généralités 154
8.2.2 Types des données et notations des messages 155
8.3 Procédure d'Association de Poste 155
8.3.1 Généralités 155
8.3.2 Certificats de clés publiques 155
8.3.3 Configuration des postes distants autorisés 158
8.3.4 Conditions préalables pour initier la procédure d'Association de Poste 158
8.3.5 Définition des messages 158
8.3.6 Diagramme d'état du poste de conduite 167
8.3.7 Diagramme d'état du poste téléconduit 180
8.3.8 Vérification du certificat du poste distant 190
8.3.9 Vérification des certificats pendant les opérations normales 191
8.3.10 Dérivation des Clés de Mise à Jour 191
8.3.11 Directives du poste de conduite pour la gestion de l'Association de Poste et des Clés de Mise à Jour 192
8.3.12 Directives du poste téléconduit pour la gestion de l'Association de Poste et des Clés de Mise à Jour 192
8.3.13 Initialisation et mise à jour d'Associations de Postes et de Clés de Mise à Jour 195
8.4 Procédure de Modification de Clé de Session 196
8.4.1 Généralités 196
8.4.2 Définition des messages 197
8.4.3 Diagramme d'état du poste de conduite 206
8.4.4 Diagramme d'état du poste téléconduit 219
8.4.5 Directives du poste de conduite pour la gestion des Clés de Session 229
8.4.6 Directives du poste téléconduit pour la gestion des Clés de Session 229
8.4.7 Initialisation et modification des Clés de Session 230
8.5 Échange de Données Sécurisées 231
8.5.1 Généralités 231
8.5.2 Définition des messages 232
8.5.3 Diagramme d'état du poste de conduite 236
8.5.4 Diagramme d'état du poste téléconduit 243
8.5.5 Directives du poste de conduite pour l'Échange de Données Sécurisées 249
8.5.6 Directives du poste téléconduit pour l'Échange de Données Sécurisées 250
8.5.7 Exemple d'Échange de Données Sécurisées pendant l'Association de Poste 250
8.5.8 Exemple d'Échange de Données Sécurisées pendant la Modification de Clé de Session 252

9 Exigences d'interopérabilité 254
9.1 Vue d'ensemble de l'article 254
9.2 Exigences minimales 254
9.2.1 Vue d'ensemble du paragraphe 254
9.2.2 Algorithmes d'authentification 254
9.2.3 Algorithmes d'enveloppement/transport de clé 254
9.2.4 Clés cryptographiques 255
9.2.5 Courbes cryptographiques 255
9.2.6 Valeurs configurables 255
9.2.7 Informations cryptographiques 257
9.3 Options 258
9.3.1 Vue d'ensemble du paragraphe 258
9.3.2 Algorithmes de MAC/AEAD 258
9.3.3 Algorithmes d'enveloppement/transport de clé 258
9.3.4 Courbes cryptographiques 259
9.4 Utilisation avec TCP/IP 259
9.5 Utilisation avec canaux redondants 259
10 Exigences de référencement de la présente norme 259
10.1 Vue d'ensemble de l'article 259
10.2 Options choisies 259
10.3 Mise en correspondance du format de message 259
10.4 Références aux procédures 260
10.5 Information de protocole 260
10.6 Réponse du poste téléconduit aux requêtes d'opérations non autorisées 260
10.7 Transmission des statistiques de sécurité 260
10.8 Valeurs configurables 260
10.9 Déclaration de conformité de la mise en œuvre d'un protocole 260
Annex A (informative) Mise en correspondance des Événements de Sécurité avec l'IEC 62351-14 261
A.1 Généralités 261
A.2 Mise en correspondance des événements définis dans l'IEC 62351-5, spécifiés dans le présent document 261
Bibliographie 263

Figure 1 – Vue d'ensemble de l'interaction entre l'Autorité Centrale et les postes 144
Figure 2 – Séquence des procédures 146
Figure 3 – Procédure d'Association de Poste 159
Figure 4 – Association de Poste – Diagramme d'état du poste de conduite 170
Figure 5 – Association de Poste – Diagramme d'état du poste téléconduit 182
Figure 6 – Exemple d'initialisation d'ID d'Association, de Clés de Mise à Jour et de Clés de Session 196
Figure 7 – Procédure de Modification de Clé de Session 197
Figure 8 – Modification de Clé de Session – Diagramme d'état du poste de conduite 209
Figure 9 – Modification de Clé de Session – Diagramme d'état du poste téléconduit 222
Figure 10 – Exemple d'initialisation et de mise à jour périodique de Clé de Session 231
Figure 11 – Échange de Données Sécurisées 232
Figure 12 – Échange de Données Sécurisées – Diagramme d'état du poste de conduite 238
Figure 13 – Échange de Données Sécurisées – Diagramme d'état du poste téléconduit 245

Figure 14 – Exemple d'Échange de Données Sécurisées pendant l'Association de Poste 251
Figure 15 – Exemple de messages de Données Sécurisées échangés pendant la Modification de Clé de Session 253

Tableau 1 – Domaine d'application aux normes 130
Tableau 2 – Résumé des clés symétriques utilisées 141
Tableau 3 – Résumé des clés asymétriques utilisées.....142
Tableau 4 – États utilisés dans le diagramme d'état du poste de conduite 147
Tableau 5 – États utilisés dans le diagramme d'état du poste téléconduit 148
Tableau 6 – Résumé des horloges et compteurs utilisés 149
Tableau 7 – Statistiques de sécurité et événements associés 150
Tableau 8 – Courbes cryptographiques elliptiques 156
Tableau 9 – Message de Requête d'Association 160
Tableau 10 – Message de Réponse d'Association 161
Tableau 11 – Message de Requête de Modification de Clé de Mise à Jour 163
Tableau 12 – Données incluses dans le calcul de MAC (dans cet ordre).....165
Tableau 13 – Message de Réponse de Modification de Clé de Mise à Jour.....166
Tableau 14 – Données incluses dans le calcul de MAC (dans cet ordre).....167
Tableau 15 – Diagramme d'état du poste de conduite: Association de Poste 171
Tableau 16 – Diagramme d'état du poste téléconduit: Association de Poste 183
Tableau 17 – Liste d'affectations rôle-permission prédéfinies 194
Tableau 18 – Message de Requête de Session.....198
Tableau 19 – Message de Réponse de Session 200
Tableau 20 – Données incluses dans le calcul MAC (dans l'ordre).....201
Tableau 20 – Message de Requête de Modification de Clé de Session 202
Tableau 21 – Données incluses dans les WKD (dans cet ordre).....204
Tableau 22 – Exemple d'ordre de Clé de Session 204
Tableau 23 – Données incluses dans le calcul de MAC (dans cet ordre).....205
Tableau 24 – Message de Réponse de Modification de Clé de Session 205
Tableau 26 – Données incluses dans le calcul de MAC (dans cet ordre).....206
Tableau 27 – Diagramme d'état du poste de conduite: Modification de Clé de Session 209
Tableau 27 – Diagramme d'état du poste téléconduit: Modification de Clé de Session 222
Tableau 28 – Message de Données Sécurisées 233
Tableau 29 – Données Utiles des Données Sécurisées utilisant un algorithme de MAC 234
Tableau 31 – Données incluses dans le calcul de MAC dans les Données Utiles des Données Sécurisées (dans cet ordre) 235
Tableau 32 – Paramètres d'algorithme de AEAD pour générer les Données Utiles des Données Sécurisées (dans cet ordre) 236
Tableau 33 – Diagramme d'état du poste de conduite: Échange de Données Sécurisées.....239
Tableau 33 – Diagramme d'état du poste téléconduit: Échange de Données Sécurisées.....246
Tableau 34 – Configuration des informations cryptographiques.....257
Tableau 35 – Légende pour la configuration des informations cryptographiques 258
Tableau A.1 – Journaux des événements d'enregistrement de sécurité définis dans l'IEC 62351-5 Éd. 1, mis en correspondance avec l'IEC 62351-14 261

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62351-5 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés. Il s'agit d'une Norme internationale.

Cette Norme internationale annule et remplace l'IEC TS 62351-5 parue en 2013. Elle constitue une révision technique. Les modifications principales présentées dans la présente Norme internationale sont les suivantes:

a) le mécanisme de communication sécurisée est réalisé par une association poste de conduite/poste téléconduit;
b) la gestion des Utilisateurs, qui sert à ajouter, modifier ou supprimer un Utilisateur, a été supprimée;
c) la méthode symétrique, qui sert à modifier la Clé de Mise à Jour, a été supprimée;

d) la méthode asymétrique, qui sert à modifier la Clé de Mise à Jour, a été révisée;

e) la procédure et les concepts de Stimulation/Réponse ont été supprimés;

f) le concept de Mode Agressif a été remplacé par le mécanisme d'échange de messages de Données Sécurisées;

g) un chiffrement authentifié des données d'application a été ajouté;

h) la liste des algorithmes de sécurité admis a été mise à jour;

i) les règles de calcul des numéros de séquence des messages ont été mises à jour;

j) la surveillance et l'enregistrement des événements ont été ajoutés.

NOTE Les caractères d'imprimerie suivants sont utilisés:

Les MAJUSCULES sont utilisées dans le texte du présent document pour identifier formellement les composantes les plus importantes du mécanisme de sécurité décrit. Ces composantes incluent: 1) les éléments relatifs aux données (par exemple, les Clés de Mise à Jour, les Clés de Session); 2) les noms de procédures (par exemple, Association de Postes, Modification de Clé de Session); les noms de message (par exemple, Requête d'Association, Requête de Session); 3) les noms d'états (par exemple, Session Établie, Attendre la Réponse de la Session); 5) les statistiques (par exemple, Erreurs d'Authentification, Messages Inattendus) et 5) les noms d'événements (par exemple, Temporisation de Réponse, Modification de Clé de Session Non Valide Rx).

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2516/FDIS	57/2555/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

1 Domaine d'application

La présente partie de l'IEC 62351 définit le mécanisme de communication sécurisée du profil d'application (profil A) qui spécifie les messages, les procédures et les algorithmes pour sécuriser le fonctionnement de tous les protocoles fondés sur ou dérivés de l'IEC 60870-5, *Matériels et systèmes de téléconduite – Protocoles de transmission*. Le présent document s'applique au moins aux protocoles énumérés dans le Tableau 1.

Tableau 1 – Domaine d'application aux normes

Numéro	Nom
IEC 60870-5-101	Norme d'accompagnement pour les tâches élémentaires de téléconduite
IEC 60870-5-102	Norme d'accompagnement pour la transmission de totaux intégrés dans un système électrique de puissance
IEC 60870-5-103	Norme d'accompagnement pour l'interface de communication d'information des équipements de protection
IEC 60870-5-104	Accès aux réseaux utilisant des profils de transport normalisés pour l'IEC 60870-5-101
DNP3	Protocole de Réseau Distribué (défini dans la norme IEEE 1815, fondé sur les normes IEC 60870-1 à IEC 60870-5 et maintenu conjointement par le Groupe d'utilisateurs du DNP et l'IEEE)

Il est prévu que les premiers lecteurs du présent document soient les membres des groupes de travail qui élaborent les protocoles énumérés dans le Tableau 1.

Pour que les mesures décrites dans le présent document entrent en application, elles doivent être acceptées et référencées par les spécifications des protocoles eux-mêmes. Le présent document est rédigé dans le but de permettre ce processus. Les groupes de travail chargés d'associer le présent document aux protocoles spécifiques énumérés dans le Tableau 1 peuvent choisir de ne pas le faire.

Il est prévu que les lecteurs suivants du présent document soient les personnes chargées d'élaborer les produits qui mettent en œuvre ces protocoles.

Certaines parties du présent document peuvent également être utiles aux gestionnaires et aux cadres dirigeants pour comprendre le but et les exigences du travail.

Ce document est organisé du plus général au plus spécifique, comme suit:

- les Articles 2 à 4 fournissent des termes, des définitions et des références de contexte;
- l'Article 5 décrit les problèmes que la présente spécification est destinée à traiter;
- l'Article 6 décrit le mécanisme de manière générale, sans référence à un protocole spécifique;
- les Articles 7 et 8 décrivent le mécanisme plus précisément. Ils constituent la partie normative principale de la présente spécification;

- l'Article 9 définit les exigences d'interopérabilité pour ce mécanisme de communication sécurisée y compris la relation entre cette norme et la CEI 62351-3 pour la sécurité de la couche transport;
- l'Article 10 décrit les exigences des autres normes qui font référence au présent document.

Il est attendu que les actions d'une organisation en réponse aux événements et conditions d'erreurs décrits dans le présent document soient définies par la politique de sécurité de l'organisme. Elles ne relèvent pas du domaine d'application du présent document.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60870-5 (toutes les parties), *Matériels et systèmes de téléconduite – Partie 5: Protocoles de transmission*

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* (disponible en anglais seulement)

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP*

IEC 62351-7, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 7: Modèles d'objets de données de gestion de réseaux et de systèmes (NSM)*

IEC 62351-8, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance*

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging* (disponible en anglais seulement)[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)*

[1] En cours d'élaboration. Stade au moment de la publication: IEC ACDV 62351-14:2021.

IETF RFC 7748, *Elliptic Curve for Security*

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

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'IEC TS 62351-2 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
ID d'Association
paire de valeurs qui identifie de manière unique la liaison de communication entre un poste de conduite et un poste téléconduit et l'ensemble de clés cryptographiques lié

3.2
autorité centrale
entité dont le domaine d'application s'étend sur toute l'organisation et dont l'objectif est de fournir des informations d'authentification aux dispositifs et systèmes de l'organisation pour les autoriser à communiquer. L'Autorité Centrale peut ou peut ne pas être également une Autorité de Certification.

3.3
liaison de communication
le canal de communication qui relie deux entités communicantes. Ce lien peut être un lien physique réel ou il peut s'agir d'un lien logique qui utilise un ou plusieurs liens physiques réels.

direction conduite
sens de la transmission depuis le poste de conduite jusqu'à un poste téléconduit

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

3.4
poste téléconduit
poste surveillé ou surveillé et commandé par un poste maître (de conduite)

Note 1 à l'article: Il est communément appelé "poste satellite" ou "poste asservi" dans certaines spécifications.

[SOURCE: IEC TR 60870-1-3:1997, modifié (remplacement de "poste de conduite" par "poste maître (de conduite)" et ajout de la Note 1 à l'article)]

3.5
poste de conduite
poste qui réalise la téléconduite de postes téléconduits

Note 1 à l'article: Il est communément appelé "poste maître" dans certaines spécifications.

[SOURCE: IEC TR 60870-1-3:1997, modifié (remplacement de "lieu d'où s'effectue" par "poste qui réalise" et de "postes satellites" par "postes téléconduits")]

3.6
poste local
poste le plus proche de l'observateur lorsque le processus est identique à la fois sur le poste de conduite et sur le poste téléconduit

3.7
direction surveillance
sens de la transmission depuis un poste téléconduit jusqu'au poste de conduite

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

3.8
poste distant
poste le plus éloigné de l'observateur lorsque le processus est identique à la fois sur le poste de conduite et sur le poste téléconduit

3.9
téléconduite
conduite à distance du fonctionnement d'une installation, utilisant la transmission d'informations à l'aide de télécommunications

Note 1 à l'article: La téléconduite peut comprendre toute combinaison de moyens de commande, d'alarme, de signalisation, de mesure, de protection et de déclenchement; l'utilisation de messages parlés est exclue.

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

4 Abréviations

Se reporter à l'IEC TS 62351-2 pour une liste des abréviations applicables. Les termes suivants sont inclus ici car ils sont utilisés spécifiquement dans les protocoles concernés ainsi que dans l'analyse de ce mécanisme de communication sécurisée.

A-Profile	(Application Profile) Profil d'Application. Sécurité pour la couche application.
AEAD	(Authenticated Encryption with Associated Data) Chiffrement Authentifié avec Données Associées. Fonction qui permet de chiffrer et d'authentifier les données (fournit confidentialité et authentification). Noter que l'AEAD comporte également une protection de l'intégrité des données supplémentaires, qui n'est pas chiffrée.
AID	(Association ID) ID d'Association. Valeur qui identifie une connexion unique entre le poste de conduite et le poste téléconduit.
ASDU	(Application Service Data Unit) Unité de Données de Service d'Application. Le message de couche application soumis aux couches inférieures pour transmission.
C.ing	(Controlling) Conduite (en référence au Poste de Conduite)
C.led	(Controlled) Téléconduit (en référence au Poste Téléconduit)
HKDF	(HMAC-based Extract-and-Expand Key Derivation Function) Fonction de Dérivation de Clé par l'utilisation de la méthode Extraire et Étendre fondée sur le HMAC. Fonction qui permet de dériver une clé cryptographique symétrique.
HMAC	(Keyed-Hash Message Authentication Code) Code d'Authentification de Message par Hachage. Fonction qui permet d'authentifier des données par l'utilisation d'une clé cryptographique secrète.
IKM	(Input Keying Material) Matériau de Modulation d'Entrée. Données fournies à la fonction HDKF-Extraire afin de générer une Clé Pseudoaléatoire (PRK).

KEK	(Key Encryption Key) Clé de Chiffrement de Clé. Clé secrète utilisée pour chiffrer une autre clé secrète.
MAC	(Message Authentication Code) Code d'Authentification de Message. Valeur calculée utilisée par un poste pour authentifier et vérifier l'intégrité d'une unité de données de protocole d'application.
PRK	(Pseudo-Random Key) Clé Pseudoaléatoire. Données fournies à la fonction HKDF-Étendre afin de générer une clé secrète.
T-Profile	(Transport Profile) Profil de Transport. Sécurité pour la couche transport (TCP/IP).
TCP/IP	(Transmission Control Protocol/Internet Protocol) Protocole de Commande de Transport/Protocole Internet.

5 Description de problème

5.1 Vue d'ensemble de l'article

L'Article 5 décrit:

- les menaces contre la sécurité que le présent document est destiné à traiter;
- les problèmes de conception propres à la mise en œuvre d'une communication sécurisée pour l'IEC 60870-5 et les protocoles dérivés;
- les principes de conception qui en découlent derrière le mécanisme.

5.2 Menaces spécifiques traitées

Le présent document ne doit traiter que les menaces contre la sécurité suivantes, telles qu'elles sont définies dans l'IEC TS 62351-2:

- usurpation;
- modification;
- rejeu;
- écoute illicite.

5.3 Problèmes de conception

5.3.1 Vue d'ensemble du paragraphe

Le paragraphe 5.3 décrit les défis à relever lors de l'élaboration d'une proposition de communication sécurisée qui peut être appliquée à l'ensemble de l'IEC 60870-5 ainsi qu'aux protocoles dérivés. Le paragraphe 5.3 est fourni à l'intention des experts de la sécurité qui révisent le présent document et qui peuvent ne pas bien connaître l'environnement du protocole du service de fourniture d'électricité.

5.3.2 Communications asymétriques

Tous les protocoles concernés par la présente spécification ont en commun le concept d'inégalité entre les postes de communication. Dans chacun de ces protocoles, il existe un poste de conduite désigné et un poste téléconduit désigné. Chacun d'entre eux a des rôles, des responsabilités, des procédures et des formats de message différents. Plus particulièrement, le poste de conduite est, dans de nombreux cas, responsable du contrôle de flux et du contrôle d'accès au support.

L'existence d'une désignation précise du poste de conduite/téléconduit a deux conséquences sur la conception de ce mécanisme de communication sécurisée:

- le format des messages dans chacune des directions est presque certainement différent, même si les fonctions sont les mêmes;
- la distribution des clés de session est simplifiée, car celles-ci sont toujours émises par le poste de conduite.

5.3.3 Orientés message

L'ensemble des protocoles concernés est orienté message. L'authentification de la connexion est effectuée une fois pour établir les clés de session, qui sont à leur tour utilisées par la suite pour prendre en charge l'authentification des messages.

L'authentification des messages doit être réalisée message par message, plutôt que de n'être réalisée qu'au début d'un flux de données puis occasionnellement par la suite, ce qui est la manière de procéder de certains protocoles orientés connexion.

5.3.4 Numéros de séquence faibles ou absence de numéros de séquence

Une technique de sécurité habituelle pour lutter contre la menace de rejeu consiste à inclure un numéro de séquence dans le message. En association avec les essais d'intégrité des messages, le numéro de séquence rend plus difficile la simulation d'utilisateur légitime par un agresseur. Celui-ci ne peut pas se contenter de copier un message existant, car les messages doivent être transmis dans un ordre précis.

Malheureusement, aucun des protocoles concernés ne comprend un numéro de séquence qui permet une protection adéquate. Les numéros de séquence qui existent ont des valeurs maximales très faibles, ce qui permet à un agresseur de tenter un rejeu après avoir recueilli un petit nombre de messages seulement.

Aussi, la conception de la présente spécification doit inclure ses propres numéros de séquence et d'autres données qui évoluent dans le temps pour fournir une protection contre le rejeu.

5.3.5 Puissance de traitement limitée

Le manque de puissance de traitement disponible dans de nombreux dispositifs de fourniture d'électricité est une source de préoccupation majeure pour la conception des protocoles concernés depuis leur création. Cette exigence de conception affecte forcément également le mécanisme de communication sécurisée. Cette préoccupation est d'autant plus forte que nombre de ces dispositifs sont des machines à processeur unique. Une attaque par déni de service affecte non seulement la capacité de communication de ces dispositifs, mais également leurs fonctions de commande, de protection ou de surveillance électriques.

Aussi, l'utilisation de mesures de sécurité qui exigent une puissance de traitement extrêmement élevée, comme le chiffrement de clés publiques et des tailles de clés très importantes, a été évitée dans toute la mesure du possible.

5.3.6 Largeur de bande limitée

La largeur de bande limitée disponible dans les réseaux de fourniture d'électricité est la principale source de préoccupation (après l'intégrité des messages) relative à la conception des protocoles concernés. Des liaisons de 1 200 bits par seconde et moins sont toujours une réalité pour de nombreuses applications de ces protocoles. Certaines liaisons de communications facturent également un service à l'octet transmis.

Aussi, le mécanisme de communication sécurisée ne doit pas ajouter une surcharge trop importante (c'est-à-dire qu'il ne doit peser que quelques octets) aux protocoles concernés. La taille des données d'authentification supplémentaires a donc été limitée et tronquée dans la mesure du possible tout en conservant un niveau de sécurité adéquat. D'autres mesures peuvent être prises pour la mise en œuvre de chaque protocole.

5.3.7 Pas d'accès au serveur d'authentification

La nature des réseaux de fourniture d'électricité dans lesquels les protocoles concernés sont mis en place fait que le poste de conduite est souvent le seul dispositif avec lequel le poste téléconduit peut communiquer. S'il existe un quelconque accès à d'autres réseaux, il est souvent réalisé au moyen du dispositif de mise en œuvre du poste de conduite.

La conséquence de cette réalité sur le mécanisme de communication sécurisée est que tout système qui exige une vérification en ligne des identifiants de sécurité du poste de conduite par une tierce partie n'est pas pratique.

5.3.8 Longueur de trame limitée

En raison des restrictions relatives à la largeur de bande et à l'intégrité des messages, les protocoles concernés sont conçus pour envoyer les données en petites trames de 255 octets ou moins. Certains protocoles dérivés permettent le "chaînage" de trames afin de créer des messages de couche application plus importants.

Toutefois, le mécanisme de communication sécurisée ne peut généralement pas prendre en charge la transmission d'unités de données importantes entre les postes.

5.3.9 Somme de contrôle limitée

L'intégrité de message a constitué une priorité élevée dans la conception des protocoles concernés. Toutefois, les mesures d'intégrité choisies pour ces protocoles ont été conçues pour protéger contre le bruit aléatoire, et pas contre une attaque concertée, comme cela est examiné ci-dessous.

- Les protocoles séries de l'IEC 60870-5 utilisent le type de trame FT1.2 qui utilise des bits de parité et une somme de contrôle à un octet unique pour protéger contre les erreurs de bits. Un octet unique n'est pas assez grand pour fournir un code d'authentification de message sécurisé (MAC).
- Le protocole de l'IEC 60870-5-104 dépend des mesures d'intégrité des couches inférieures. Comme la présente spécification examine seulement un mécanisme de couche application, celui-ci ne peut dépendre de telles mesures. De toute façon, s'il est procédé ainsi, la solution ne vaut que pour un seul des protocoles concernés.
- Le protocole DNP3 utilise la trame FT3 de l'IEC 60870-5, avec une vérification de redondance cyclique à deux octets tous les 16 octets ou moins. Ceci fournit une intégrité importante, si ce n'est qu'aucune vérification n'est effectuée sur la totalité de la trame.

Aussi, le mécanisme de communication sécurisée décrit dans la présente norme ne peut pas utiliser les mécanismes d'intégrité de protocole existants pour fournir l'intégrité des messages dans un but de sécurité.

5.3.10 Systèmes radio

Les protocoles concernés sont souvent utilisés sur des systèmes radio qui peuvent ou peuvent ne pas fournir leurs propres mesures de sécurité. De nombreux réseaux radio de fourniture d'électricité ne fournissent aucune sécurité.

Aussi, le mécanisme décrit dans la présente norme doit prendre pour hypothèse un environnement de transmission hostile et non sécurisé sur le plan physique.

5.3.11 Systèmes commutés

Les protocoles concernés sont fréquemment utilisés sur des réseaux téléphoniques commutés qui exigent plusieurs secondes de délai pour établir de nouveau la communication avant la transmission de chaque trame. De même, de nombreux systèmes radio exigent des temps de "modulation" longs avant chaque trame.

Par conséquent, l'extension de sécurité décrite dans la présente norme utilise toujours une méthode d'authentification de tous les messages de données d'application, dénommée "mode agressif", qui réduit le nombre de trames de données supplémentaires à transmettre.

5.3.12 Diversité des protocoles concernés

La famille de protocoles IEC 60870-5 partage de nombreuses fonctions communes et une philosophie de conception sous-jacente. Toutefois, les différentes normes d'accompagnement et les protocoles dérivés ont été mis en œuvre par une diversité de formats de messages et de procédures.

Aussi, la présente spécification décrit un mécanisme de communication sécurisée générique qui doit être mis en correspondance avec chaque protocole concerné spécifique dans le contexte des spécifications qui sont particulières à ce protocole.

5.3.13 Couches liaison de données différentes

Comme cela est examiné en 5.3.9, les protocoles concernés utilisent une diversité de mécanismes et de procédures de transport. Bien que l'IEC 60870-5 décrive une couche liaison de données commune, elle permet des formats de trames multiples et d'autres options. Plusieurs des protocoles concernés utilisent la trame FT1.2, l'un d'entre eux utilise la trame FT3 et un autre n'utilise pas du tout ce format de trame. Certains d'entre eux utilisent uniquement une procédure de contrôle d'accès au support asymétrique, certains utilisent une méthode symétrique, et d'autres utilisent les deux de manière facultative.

Aussi, le mécanisme de communication sécurisée ne peut pas être fondé sur la couche liaison de données. Toutefois, il peut prendre pour hypothèse que l'information d'adressage est disponible dans les couches inférieures et peut être utilisée pour l'authentification.

5.3.14 Intervalles d'amélioration longs

Les fournisseurs d'électricité amortissent les modifications apportées à leurs réseaux sur des périodes longues et ils peuvent déployer plusieurs générations différentes de systèmes de réseau en même temps.

Aussi, ce mécanisme de communication sécurisée suit les principes décrits en 5.4.

5.3.15 Sites à distance

Les dispositifs qui mettent en œuvre les protocoles concernés se trouvent souvent dans des sites très éloignés et dont l'accès est onéreux.

Aussi, dans toute la mesure du possible, ce mécanisme comprend des méthodes qui permettent de mettre à jour à distance les identifiants de sécurité.

5.3.16 Supports peu fiables

Les protocoles concernés sont souvent utilisés sur des supports peu fiables. Ce mécanisme cherche à prendre en compte ce manque de fiabilité lors du traitement des conditions d'erreur. Par exemple, il ne considère pas par hypothèse que la perte d'un message unique signifie forcément qu'une attaque est en cours.

5.4 Principes généraux

5.4.1 Vue d'ensemble du paragraphe

Le paragraphe 5.4 décrit les principes directeurs du présent document, fondés sur les menaces et les problèmes de conception identifiés examinés dans les deux articles précédents.

5.4.2 Couche application seulement

Le présent document décrit la communication sécurisée comme un profil A. Se reporter à l'IEC 62351-1 pour une analyse des raisons pour lesquelles la sécurité entre applications est nécessaire dans le contexte des fournisseurs d'électricité, en complément de la sécurité de couche transport qui peut être mise en œuvre.

5.4.3 Définition générique mise en correspondance avec différents protocoles

Le présent document décrit une méthode commune de chiffrement qui peut être utilisée par tout protocole concerné. La mise en œuvre de cette méthode dans chaque protocole doit être définie par des normes séparées. De telles normes doivent faire référence au présent document selon les règles définies à l'Article 10.

5.4.4 Bidirectionnel

Le présent document décrit un mécanisme qui peut être utilisé dans les deux sens de transmission, malgré l'asymétrie du trafic des communications définie par les protocoles concernés et examinée en 5.3.2.

5.4.5 Gestion des clés cryptographiques

Le présent document fournit la méthode pour modifier à distance les clés qui utilisent une combinaison de chiffrement asymétrique (à clé publique) et de chiffrement symétrique afin de gérer les identifiants de sécurité.

Le présent document utilise de nombreux niveaux de clés pour les raisons suivantes:

- une Clé de Session symétrique modifiée périodiquement est utilisée pour fournir une protection contre les attaques par force brute et limite la puissance informatique exigée;
- une Clé de Mise à Jour symétrique modifiée occasionnellement est utilisée pour renouveler les Clés de Session;
- une paire de clés asymétrique détenue par chaque dispositif est utilisée pour modifier les Clés de Mise à Jour, car il est plus simple de les gérer et de les distribuer sous forme de certificats.

5.4.6 Rétrotolérance

Le présent document recommande que les conditions suivantes soient satisfaites lorsqu'un dispositif sécurisé (un dispositif qui met en œuvre ce mécanisme de communication sécurisée) communique avec un dispositif non sécurisé:

- il convient que le dispositif sécurisé soit capable de détecter que le dispositif non sécurisé ne prend pas en charge le mécanisme de communication sécurisée;
- il convient que le dispositif non sécurisé continue à fonctionner normalement après avoir été contacté par le dispositif sécurisé. Autrement dit, le message d'authentification ne peut pas entraîner la défaillance du dispositif non sécurisé.

5.4.7 Possibilité de mise à jour

Le présent document permet aux administrateurs de système de modifier les algorithmes ainsi que d'autres paramètres de sécurité afin de prendre en compte les exigences à venir. Conformément au principe d'interopérabilité entre les dispositifs, il permet également de mettre à jour une liaison une extrémité à la fois.

5.4.8 Connexions multiples

Le présent document prend pour hypothèse qu'il peut y avoir plusieurs postes de conduite connectés au même poste téléconduit qui communiquent en même temps. Il fournit une méthode pour identifier et authentifier chacun des postes de conduite connectés, séparément les uns des autres, quelles que soient les informations concernant leur adresse.

L'ID d'Association examinée dans le présent document permet d'identifier chaque liaison de communication dans le système comme une association de postes de conduite/téléconduit. Elle permet également que les postes téléconduits puissent imiter l'accès à certaines fonctions selon des "rôles" et des "droits" (RBAC) assignés au poste de conduite.

Cette information peut être utilisée pour créer une piste d'audit à des fins de sécurité. Il convient que les personnes qui la mettent en œuvre prennent note du fait que l'enregistrement et la vérification d'événements de sécurité tels que les Erreurs d'Authentification constituent une partie cruciale de la sécurité des informations. Il est recommandé que toutes les mises en œuvre enregistrent au moins toutes les authentifications, réalisées avec succès ou non, et les modifications de clés, comprenant l'heure, les adresses et la liaison de communication concernée. Afin d'obtenir les meilleurs résultats d'analyse, il convient que les postes enregistrent des messages entiers, y compris l'ensemble des informations d'authentification, afin qu'un auditeur puisse évaluer l'authenticité des messages.

6 Théorie de fonctionnement

6.1 Vue d'ensemble de l'article

L'Article 6 décrit le fonctionnement du mécanisme de communication sécurisée en général à l'intention des personnes qui lisent la norme pour la première fois. Dans le cas où le présent article et l'Article 7 divergent, l'Article 7 doit être considéré comme la version correcte.

6.2 Communication sécurisée

6.2.1 Concepts fondamentaux

6.2.1.1 Présentation

La communication sécurisée définie dans le présent document est fondée sur l'authentification et le chiffrement facultatif des données transmises par la liaison de communication au moyen de clés cryptographiques.

6.2.1.2 Mode d'authentification seulement

Lorsque le mode d'authentification seulement est utilisé, le mécanisme de communication sécurisée est fondé sur le concept d'un Code d'Authentification de Message (MAC) que les postes de conduite et téléconduit calculent pour chaque Unité de Données de Service d'Application (ASDU, ou message de protocole) qui doit être authentifiée.

Un algorithme de MAC est un calcul mathématique qui prend pour éléments d'entrée une clé symétrique et le message de protocole, produit une donnée plus petite comme élément de sortie et présente les caractéristiques suivantes:

- la fonction MAC prend pour éléments d'entrée la clé et le message de protocole et produit le marqueur d'authentification;
- la valeur de sortie est sensible à de petites variations du message d'entrée. La sortie du MAC peut donc être utilisée pour détecter si le message a été modifié;
- le calcul utilise de manière intrinsèque une clé secrète partagée par les deux extrémités de la communication;

- il est extrêmement difficile de déterminer la clé secrète par l'observation du message et de la sortie du MAC;
- il est pratiquement impossible de déterminer le message originel à partir du MAC;
- il est difficile de trouver deux messages qui produisent le même MAC.

6.2.1.3 Mode de chiffrement authentifié

En cas d'utilisation d'un mode authentifié et chiffré, le mécanisme de communication sécurisée est fondé sur le concept de chiffrement authentifié avec des données supplémentaires (AEAD). Il s'agit d'une forme de chiffrement qui assure la confidentialité et l'authenticité des données de manière simultanée, au moyen d'une clé de chiffrement symétrique et d'un marqueur d'authentification. Le marqueur d'authentification peut comprendre en outre des informations issues de données supplémentaires qui peuvent être transmises sous forme de texte en clair (et qui ne sont donc pas confidentielles).

Un AEAD présente les caractéristiques suivantes:

- le texte en clair à chiffrer, le texte en clair à utiliser comme données supplémentaires, une clé symétrique et un nonce constituent les entrées de la fonction de chiffrement;
- le texte chiffré et un marqueur d'authentification constituent les sorties de la fonction de chiffrement;
- la clé symétrique, le nonce, les données supplémentaires, le texte chiffré et le marqueur d'authentification constituent les entrées de la fonction de déchiffrement;
- une valeur booléenne qui indique la réussite ou non de l'authentification et le texte en clair intégré à l'origine dans la fonction de chiffrement (sous réserve de la réussite de l'authentification) constituent les sorties de la fonction de déchiffrement;
- le marqueur d'authentification, comme un MAC, est extrêmement sensible à de légères modifications de l'entrée. Il peut donc être utilisé pour détecter si le message (y compris les données supplémentaires en clair) a été modifié;
- il est extrêmement difficile de déterminer soit la clé secrète soit le texte en clair à partir de la sortie de la fonction;
- il est extrêmement difficile d'identifier deux messages qui produisent le même marqueur d'authentification.

6.2.2 ID d'Association

Dans ce mécanisme de communication sécurisée, chaque liaison de communication est identifiée par une ID d'Association numérique. L'ID d'Association est composée de l'ID d'Association du poste de conduite et de l'ID d'Association du poste téléconduit concaténées. À chaque association correspond un ensemble de clés cryptographiques utilisées pour chiffrer et/ou authentifier les informations échangées. Les clés cryptographiques sont décrites en 6.2.6.

6.2.3 Authentification

Lorsqu'il reçoit un message qui contient des informations d'authentification, le récepteur réalise le même calcul avec les mêmes données que celles utilisées par l'émetteur. Si les résultats correspondent, le récepteur permet la poursuite des communications. Si l'émetteur protégeait une ASDU particulière (données d'application), le récepteur doit traiter cette ASDU.

Si l'authentification échoue, le récepteur n'utilise pas les données contenues dans le message reçu et le message doit être ignoré. Si le récepteur est un poste téléconduit, il ne réalise pas l'opération demandée dans le message.

6.2.4 Autorité Centrale

Il convient de ne confier la capacité d'ajouter ou de supprimer un poste du système à aucun utilisateur particulier d'un poste de conduite. Il convient que cette fonction soit exécutée par du personnel autorisé ou par une Autorité Centrale dont le domaine de compétence s'étend sur toute l'organisation. L'Autorité Centrale peut ou peut ne pas être également une Autorité de Certification. La spécification de la fonctionnalité complète de l'Autorité Centrale ne relève pas du domaine d'application du présent document.

6.2.5 Contrôle d'Accès Basé sur les Rôles (RBAC)

Dans ce mécanisme de communication sécurisée, un rôle spécifique ou plus peut être assigné au poste de conduite conformément à l'IEC 62351-8. Chaque rôle est autorisé à réaliser un ensemble spécifique d'opérations sur le poste téléconduit. Le poste téléconduit vérifie que le rôle assigné au poste de conduite lui permet de réaliser l'opération demandée.

L'assignation des rôles au poste de conduite doit être réalisée par le personnel autorisé ou par l'Autorité Centrale.

6.2.6 Clés cryptographiques

6.2.6.1 Généralités

Le Tableau 2 et le Tableau 3 résument l'utilisation et la mise à jour des clés cryptographiques dans ce mécanisme de communication sécurisée. Les clés sont gérées par le poste téléconduit et le poste de conduite au moins. De manière facultative, une tierce partie de confiance connue comme Autorité Centrale peut gérer les certificats et les politiques utilisées pour la gestion des clés.

Tableau 2 – Résumé des clés symétriques utilisées

Type	Utilisation	Mécanisme de modification	Plage d'intervalle de modification attendue
Clé de Session de direction surveillance	Utilisée pour authentifier et chiffrer éventuellement les données transmises dans la direction surveillance par le poste téléconduit.	Le poste de conduite enveloppe les Clés de Session de Direction surveillance et de Direction conduite à l'aide de la Clé de Mise à Jour de Chiffrement et transmet les Clés de Session enveloppées dans un message de Modification de Clé de Session authentifié par la Clé de Mise à Jour d'Authentification.	Minutes à semaines
Clé de Session de Direction conduite	Utilisée pour authentifier et chiffrer éventuellement les données transmises dans la direction conduite par le poste de conduite.	Le poste de conduite enveloppe les Clés de Session de Direction surveillance et de Direction conduite à l'aide de la Clé de Mise à Jour de Chiffrement et transmet les Clés de Session enveloppées dans un message de Modification de Clé de Session authentifié par la Clé de Mise à Jour d'Authentification.	Minutes à semaines
Clé de Mise à Jour d'Authentification	Clé symétrique utilisée à la fois par le poste de conduite et le poste téléconduit pour authentifier la Clé de Mise à Jour de Chiffrement et les Clés de Session lorsqu'elles sont modifiées périodiquement.	La Clé de Mise à Jour d'Authentification est générée et fait l'objet d'un accord entre les deux postes au moyen d'un échange des mécanismes Diffie-Hellman basés sur une courbe elliptique (ECDH) et d'une Fonction de Dérivation de Clé par l'utilisation de la méthode Extraire et Étendre fondée sur le HMAC (HKDF).	Mois ou années

Type	Utilisation	Mécanisme de modification	Plage d'intervalle de modification attendue
Clé de Mise à Jour de Chiffrement	Clé symétrique utilisée par le poste de conduite et le poste téléconduit respectivement, pour envelopper et développer les Clés de Session lorsqu'elles sont modifiées périodiquement.	La Clé de Mise à Jour Chiffrement est générée et fait l'objet d'un accord entre les deux postes au moyen d'un échange des mécanismes Diffie-Hellman basés sur une courbe elliptique (ECDH) et d'une Fonction de Dérivation de Clé par l'utilisation de la méthode Extraire et Étendre fondée sur le HMAC (HKDF).	Mois ou années

Tableau 3 – Résumé des clés asymétriques utilisées

Type	Utilisation	Mécanisme de modification	Plage d'intervalle de modification attendue
Clé Privée de l'Autorité Centrale	L'Autorité Centrale qui agit comme une Autorité de Certification utilise sa Clé Privée pour certifier la Clé Publique d'un dispositif.	La Clé Privée de l'Autorité Centrale est gardée secrète par cette dernière et ne peut être modifiée que par des moyens externes au protocole.	Années, si cela se produit
Clé Publique de l'Autorité Centrale	Le poste local utilise la Clé Publique de l'Autorité Centrale pour valider le certificat de Clé Publique du poste distant.	La Clé Publique de l'Autorité Centrale est contenue dans un Certificat de Clé Publique. Elle peut être transmise n'importe où en clair, mais elle doit être installée en sécurité dans le poste de contrôle et dans le poste téléconduit par du personnel de confiance.	Années, si cela se produit
Clé Privée du Poste	Le poste local utilise sa Clé Privée pour remplir l'Agrément de Clés de Mise à Jour avec le poste distant	Il convient que la Clé Privée du poste soit générée par le poste lui-même et stockée en sécurité dans le dispositif, ou elle doit être installée et stockée en sécurité dans le poste par du personnel de confiance.	Années, si cela se produit
Clé Publique du Poste	Le poste local utilise la Clé Publique du poste distant pour remplir l'Agrément de Clés de Mise à Jour avec le poste distant.	Il convient que la Clé Publique du poste soit générée par le poste proprement dit. Elle est par ailleurs contenue dans un Certificat de Clé Publique qui peut être transmis n'importe où en clair. Si la paire de clés publique/privée et le certificat sont générés par une Autorité Centrale, elle doit être installée et stockée en sécurité dans le poste par du personnel de confiance.	Années, si cela se produit

De plus amples informations sur la gestion et la dérivation de clés peuvent être consultées dans l'IEC 62351-9.

6.2.6.2 Clés de Session

Les Clés de Session sont les clés utilisées le plus fréquemment. Chaque poste utilise les Clés de Session pour authentifier ou chiffrer et authentifier les données d'application envoyées et reçues.

Il existe deux Clés de Session différentes: l'une utilisée pour authentifier les données dans la direction surveillance, et l'autre utilisée pour authentifier les données transmises dans la direction conduite, de manière que, si la clé utilisée dans l'une des directions est compromise, elle ne compromette pas les communications dans l'autre direction.

Il existe un ensemble différent de Clés de Session pour chaque Association de poste de conduite/poste téléconduit, identifiée par l'ID d'Association.

Les Clés de Session d'une Association ne peuvent être initialisées et modifiées par la suite que si les Clés de Mise à Jour ont auparavant été initialisées pour la même Association par l'exécution de la procédure d'Association de Poste, définie en 8.3.

Le poste de conduite initialise les Clés de Session immédiatement après que les communications sont établies si les Clés de Session ne sont pas valides, et modifie les Clés de Session régulièrement par la suite. La modification périodique des Clés de Session les protège contre le fait d'être compromises par une analyse de la liaison de communications.

Les Clés de Session sont modifiées périodiquement par l'application de la procédure de Modification de Clé de Session définie en 8.4. Dans cette procédure, les Clés de Session sont enveloppées et authentifiées par le poste de conduite au moyen des Clés de Mise à Jour et transmises au poste téléconduit. L'utilisation d'une deuxième paire de clés, les Clés de Mise à Jour, permet au poste de conduite de modifier les Clés de Session même si les Clés de Session initiales ont été compromises. Les Clés de Session ainsi que les Clés de Mise à Jour sont des clés symétriques.

Il est primordial pour la sécurité que chaque dispositif garde les Clés de Session secrètes. Le mécanisme utilisé pour cela ne relève pas du domaine d'application du présent document, mais il convient que les personnes chargées de sa mise en œuvre prennent note du fait que si les Clés de Session sont stockées dans le dispositif de manière non sécurisée, l'intégralité du mécanisme de communication sécurisée est compromise.

Noter que si les Clés de Session sont stockées dans une mémoire non volatile, des dispositifs doivent assurer que les mêmes numéros de séquence dans les messages ne sont pas réutilisés avec les mêmes Clés de Session, et que l'expiration des Clés de Session due au délai ou au compteur d'utilisation est toujours respectée.

6.2.6.3 Clés de Mise à Jour

Les Clés de Mise à Jour sont des clés symétriques:

– la Clé de Mise à Jour de Chiffrement est une Clé de Chiffrement de Clé (KEK) utilisée pour envelopper les Clés de Session sur le poste de conduite et pour développer les Clés de Session sur le poste téléconduit;
– la Clé de Mise à Jour d'Authentification est utilisée pour authentifier la procédure d'Association de Poste décrite en 8.3 et la procédure de Modification de Clé de Session décrite en 8.4.

Il existe un ensemble différent de Clés de Session pour chaque Association de poste de conduite/poste téléconduit. Pour chaque Association, le poste de conduite peut se voir assigné à un Rôle qui désigne les actions spécifiques qu'il lui est permis d'entreprendre.

Les Clés de Mise à Jour de chaque ID d'Association sont initialisées et modifiées par la réalisation de la procédure d'Association de Poste décrite en 8.3.

L'Agrément de Clés de Mise à Jour entre le poste de conduite et le poste téléconduit est réalisé pour la première fois pendant la phase d'enregistrement du poste après l'installation ou le remplacement du poste.

Les Clés de Mise à Jour sont rarement modifiées. La justification d'une telle modification dépend de la politique de sécurité de l'organisation, mais elle peut inclure le fait que les Clés de Mise à Jour sont compromises, ou lorsque le Rôle du poste de conduite est modifié. La méthode utilisée pour agréer les Clés de Mise à Jour est fondée sur la cryptographie asymétrique (clé publique).

Il est primordial pour la sécurité que chaque dispositif garde les Clés de Mise à Jour secrètes. Le mécanisme utilisé pour cela ne relève pas du domaine d'application du présent document, mais il convient que les personnes chargées de sa mise en œuvre prennent note du fait que si les Clés de Mise à Jour sont stockées dans le dispositif de manière non sécurisée, l'intégralité du mécanisme de communication sécurisée est compromise.

Les Clés de Mise à Jour qui ont fait l'objet d'un accord pendant la procédure d'Association de Poste doivent être stockées de manière permanente sur chaque poste, de telle manière que cette procédure ne doit pas être exécutée après l'initialisation d'un poste ou après un échec de communication.

6.2.6.4 Clés publiques et privées du poste

Les clés publiques et privées du poste sont utilisées pour convenir des Clés de Mise à Jour. Dans ce but, le poste de conduite et le poste téléconduit échangent leur clé publique. Cette méthode exige l'utilisation de certificats de clé publique. Le certificat est fourni au poste lorsque le poste doit être ajouté ou remplacé dans le système ou lorsqu'il convient que son Rôle soit modifié.

Comme le représente la Figure 1, la tâche du poste (de conduite ou téléconduit) se limite généralement à transmettre son certificat de clés publiques à l'autre poste connecté et autorisé à communiquer, et à vérifier que les nouvelles Clés de Mise à Jour assignées à l'association de poste de conduite/téléconduit correspondante sont agréées de manière sécurisée.

Les communications entre le poste et l'Autorité Centrale dans le but de certifier le poste lui-même ne relèvent pas du domaine d'application du présent document, mais doivent également être sécurisées. De plus amples informations sur la gestion des certificats peuvent être consultées dans l'IEC 62351-9.

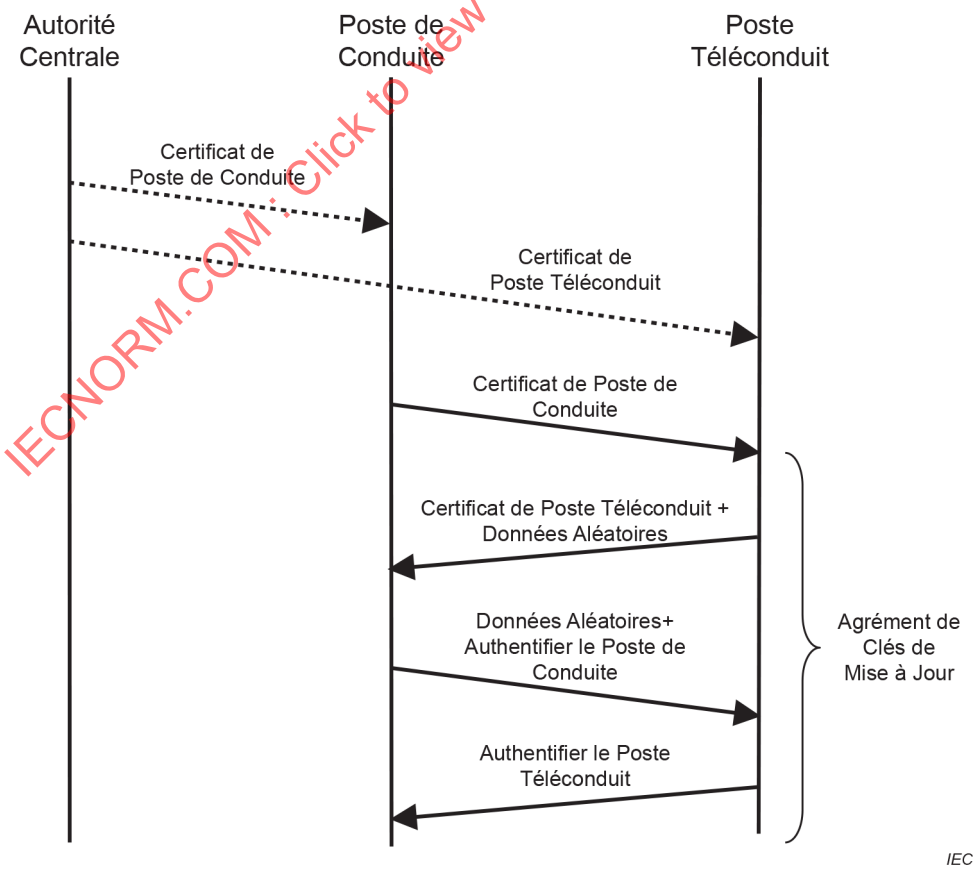


Figure 1 – Vue d'ensemble de l'interaction entre l'Autorité Centrale et les postes

6.2.7 Statistiques de sécurité

L'une des caractéristiques importantes du mécanisme de communication sécurisée est qu'il permet aux opérateurs du réseau de détecter certains types d'attaques. Tout poste téléconduit qui met en œuvre cette communication sécurisée doit garder des statistiques concernant le fonctionnement des diagrammes d'états de protocole et consigner ces statistiques comme partie intégrante du fonctionnement normal du protocole concerné. Si certaines statistiques (par exemple, les erreurs d'authentification) se mettent à dépasser fréquemment les seuils de consignation des événements, cela peut indiquer qu'une attaque est en cours. Les postes téléconduits peuvent communiquer des statistiques de sécurité aux postes de conduite autres que celles impliquées dans la communication sécurisée. Cette opération permet aux opérateurs du réseau de détecter des attaques qui peuvent être en cours sur d'autres liaisons que celle qu'ils sont en train de surveiller.

6.2.8 Événements de sécurité

Il est important de porter une attention particulière à l'enregistrement des violations liées à la sécurité dans un journal séparé, dont le contenu est par nature à l'abri de la manipulation (par exemple, la modification des informations ou la suppression d'informations). Il convient que les personnes qui en assurent la mise en œuvre s'efforcent d'archiver suffisamment d'informations pour que l'audit de sécurité et ses suites soient facilités. La mise en œuvre effective de la présente recommandation est un sujet local.

Les communications et les définitions appropriées relatives à la surveillance et l'enregistrement de sécurité sont traitées dans deux parties distinctes de l'IEC 62351: l'IEC 62351-7 traite de la surveillance de sécurité dans le contexte de la gestion de réseau, tandis que l'IEC 62351-14 traite de l'enregistrement de sécurité.

7 Exigences fonctionnelles

7.1 Vue d'ensemble de l'article

L'Article 7 décrit de manière formelle les fonctionnalités exigées par ce mécanisme de communication sécurisée. Dans le cas où l'Article 7 et l'Article 6 divergent, l'Article 7 doit être considéré comme prioritaire.

Les dispositifs dont la conformité au présent document est revendiquée doivent mettre en œuvre le mécanisme de communication sécurisée décrit à l'Article 7 indépendamment pour chaque Association entre un poste de conduite et un poste téléconduit.

7.2 Vue d'ensemble des procédures

Le mécanisme de communication sécurisée défini dans le présent document se compose de trois procédures:

a) Association de Poste

   Réalisée pour créer et mettre à jour une association entre poste de conduite/poste téléconduit avec le rôle du poste de conduite et les Clés de Mise à Jour correspondantes.

b) Modification de Clé de Session

   Exécutée après l'Association de Poste, et renouvelle régulièrement les Clés de Session au moyen des Clés de Mise à Jour.

c) Échange de Données Sécurisées

   Il s'agit de l'état de fonctionnement dans lequel les postes authentifient et échangent les données d'application. Les données d'application sont sécurisées au moyen des Clés de Session.

La Figure 2 représente la séquence d'exécution de ces procédures.

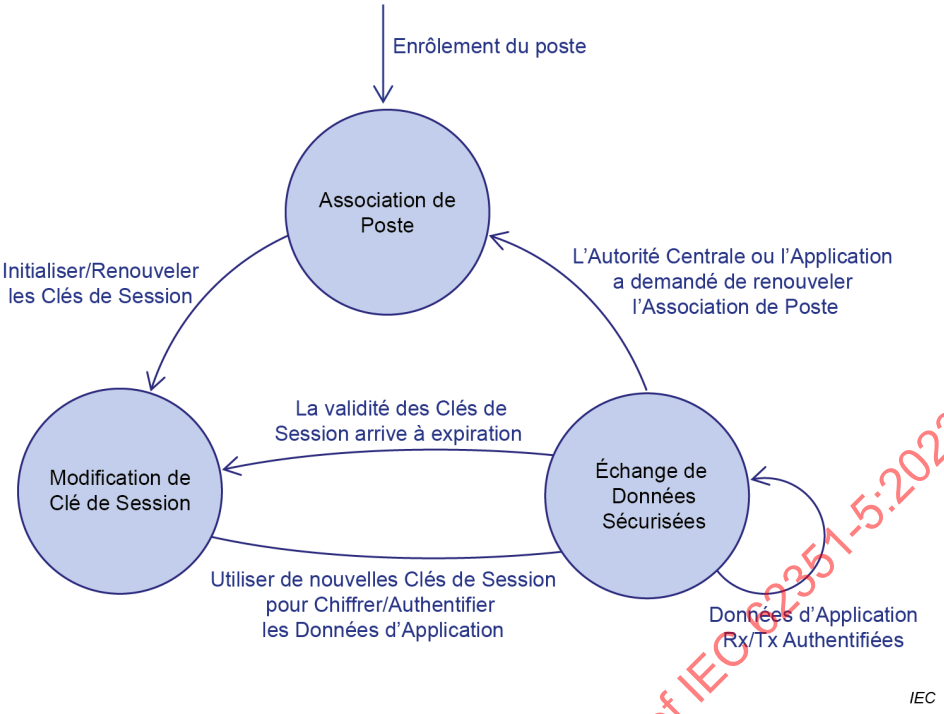


Figure 2 – Séquence des procédures

7.3 Vue d'ensemble des diagrammes d'états

Le Tableau 4 et le Tableau 5 décrivent les états utilisés par les diagrammes d'états dans ces procédures, dans l'ordre général dans lequel il peut être attendu qu'ils se produisent.

Comme cela est décrit dans les tableaux de diagrammes d'états, certains états d'Association de Poste et de Modification de Clé de Session sont seulement momentanés et les diagrammes d'états reviennent immédiatement à leur état stable après avoir entrepris les actions appropriées.

Il convient que le poste de conduite n'exécute pas simultanément la procédure d'Association de Poste et la procédure de Modification de Clé de Session. Pour cette raison, les diagrammes d'états Association de Poste et Modification de Clé de Session partagent l'état stable.

Le diagramme d'état doit être indépendant pour chaque liaison de communication avec les postes distants (identifié par le ID d'Association), aussi bien dans le poste de conduite que dans le poste téléconduit.

Tableau 4 – États utilisés dans le diagramme d'état du poste de conduite

État	Procédure	Description
État Inactif de Gestion de Clés	Association de Poste Modification de Clé de Session	Cet état stable est partagé entre les diagrammes d'états Association de Poste et Modification de Clé de Session. Il s'agit de l'état dans lequel le poste de conduite n'est pas sollicité pour exécuter la procédure d'Association de Poste ou la procédure de Modification de Clé de Session. Les Clés de Mise à Jour et les Clés de Session peuvent être valides ou non valides.
Attendre la Réponse d'Association	Association de Poste	Le diagramme d'état Association de Poste entre dans cet état transitoire lorsque le poste de conduite a transmis une Requête d'Association et est en attente de la Réponse d'Association du poste téléconduit.
Attendre la Réponse de Modification de Clé de Mise à Jour.	Association de Poste	Le diagramme d'état Association de Poste entre dans cet état transitoire lorsque le poste de conduite a transmis une Requête de Modification de Clé de Mise à Jour et est en attente de la Réponse de Modification de Clé de Mise à Jour du poste téléconduit.
Attendre la Réponse de Session	Modification de Clé de Session	Le diagramme d'état Modification de Clé de Session entre dans cet état transitoire lorsque le poste de conduite a transmis une Requête de Session et est en attente de la Réponse de Session du poste téléconduit.
Attendre la Réponse de Modification de Clé de Session.	Modification de Clé de Session	Le diagramme d'état Modification de Clé de Session entre dans cet état transitoire lorsque le poste de conduite a transmis une Requête de Modification de Clé de Session et est en attente de la Réponse de Modification de Clé de Session du poste téléconduit.
Pas de Session	Échange de Données Sécurisées	Le diagramme d'état Échange de Données Sécurisées entre dans cet état stable si les clés de Session ne sont PAS valides. Dans cet état, le poste de conduite ne peut pas échanger des messages de Données Sécurisées avec le poste téléconduit.
Session Établie	Échange de Données Sécurisées	Le diagramme d'état Échange de Données Sécurisées entre dans cet état stable si les clés de Session sont valides. Dans cet état, le poste de conduite échange des messages de Données Sécurisées avec le poste téléconduit.
Transmission des Données Sécurisées interrompue.	Échange de Données Sécurisées	Le diagramme d'état Échange de Données Sécurisées entre dans cet état transitoire lorsque la transmission des messages de Données Sécurisées est interrompue par le diagramme d'état Modification de Clé de Session. Dans cet état, le message de Données Sécurisées peut être reçu, mais non transmis.

Tableau 5 – États utilisés dans le diagramme d'état du poste téléconduit

État	Procédure	Description
État inactif d'Association	Association de Poste	Il s'agit de l'état stable dans lequel il n'est pas demandé au poste téléconduit d'exécuter la procédure d'Association de Poste par l'intermédiaire du poste de conduite. Les Clés de Mise à Jour peuvent être valides ou non valides.
Attendre la Requête de Modification de Clé de Mise à Jour.	Association de Poste	Le diagramme d'état Association de Poste entre dans cet état transitoire lorsque le poste téléconduit a transmis une Réponse d'Association et est en attente de la Requête de Modification de Clé de Mise à Jour du poste de conduite.
Pas d'Association	Modification de Clé de Session	Le diagramme d'état Modification de Clé de Session entre dans cet état stable si les clés de Mise à Jour ne sont PAS valides. La Modification de Clé de Session ne peut pas être exécutée.
État Inactif de Session	Modification de Clé de Session	Le diagramme d'état Modification de Clé de Session entre dans cet état stable si les clés de Mise à Jour sont valides. La Modification de Clé de Session peut être exécutée.
Attendre la Requête de Modification de Clé de Session.	Modification de Clé de Session	Le diagramme d'état Modification de Clé de Session entre dans cet état transitoire lorsque le poste téléconduit a transmis une Réponse de Session et est en attente de la Requête de Modification de Clé de Session du poste de conduite.
Pas de Session	Échange de Données Sécurisées	Le diagramme d'état Échange de Données Sécurisées entre dans cet état stable si les clés de Session ne sont PAS valides. Dans cet état, le poste téléconduit ne peut pas échanger des messages de Données Sécurisées avec le poste de conduite
Session Établie	Échange de Données Sécurisées	Le diagramme d'état Échange de Données Sécurisées entre dans cet état stable si les clés de Session sont valides. Dans cet état, le poste téléconduit échange des messages de Données Sécurisées avec le poste de conduite.

7.4 Horloges et compteurs

Ce mécanisme de communication sécurisée utilise différentes horloges et différents compteurs pour contrôler l'exécution des procédures décrites à l'Article 8. Le Tableau 6 donne un résumé de ces horloges et compteurs, indique la manière dont ils sont utilisés, ainsi que les seuils correspondants et les événements liés.

Tableau 6 – Résumé des horloges et compteurs utilisés

Nom	Utilisation	Type de poste	Seuil	Événement dans le diagramme d'état
Horloge de réponse	Le poste de conduite utilise cette horloge pour vérifier que, lorsqu'une requête a été envoyée, la réponse correspondante est reçue dans le temps prévu.	Conduite	Temps de Réponse Prévu	Temporisation de réponse
Horloge de requête	Le poste téléconduit utilise cette horloge pour vérifier qu'une requête spécifique est reçue dans le temps prévu. Dans le poste téléconduit, le diagramme d'état Association de Poste et le diagramme d'état Modification de Clé de Session doivent utiliser deux Horloges de Requête indépendantes.	Téléconduit	Temps de Requête Prévu	Temporisation de requête
Horloge d'utilisation de Clé de Session	Le poste utilise cette horloge pour vérifier le temps pendant lequel la Clé de Session a été utilisée pour authentifier les Messages de Données Sécurisées depuis l'exécution réussie de la dernière procédure de Modification de Clé de Session.	Conduite et téléconduit	Temps maximal d'Utilisation de Clé de Session	Expiration du Temps d'Utilisation de Clé de Session
Compteur d'Utilisation de Clé de Session	Le poste utilise ce compteur pour vérifier le nombre de fois que la Clé de Session a été utilisée pour authentifier les Messages de Données Sécurisées depuis l'exécution réussie de la dernière procédure de Modification de Clé de Session. Ce compteur est incrémenté de 1 à chaque traitement réussi d'un Message de Données Sécurisées.	Conduite et téléconduit	Compte maximal d'Utilisation de Clé de Session	Dépassement du Compte d'Utilisation de Clé de Session

Chaque poste doit permettre la configuration des seuils des Horloges/Compteurs énumérés dans le Tableau 6. L'unité de mesure et les plages configurables de ces seuils sont définies dans les exigences d'interopérabilité en 9.2.6 du présent document.

7.5 Statistiques de sécurité et événements

7.5.1 Généralités

Les postes doivent surveiller l'utilisation de ce mécanisme de communication sécurisée en faisant le compte d'un certain nombre d'événements de protocole à l'aide de compteurs de statistiques de sécurité. Pour chaque événement, le poste doit permettre les comptes de statistiques de sécurité jusqu'à 4294967295 (32 bits). Le Tableau 7 résume les statistiques de sécurité et décrit l'événement dont le compte est fait.

Les tableaux de diagrammes d'états de ce mécanisme de communication sécurisée décrivent les conditions précises dans lesquelles les statistiques doivent être incrémentées, et les actions spécifiques à entreprendre. Le Total des Messages Envoyés et le Total des Messages Reçus, qui sont incrémentés trop fréquemment pour être documentés de manière spécifique, constituent l'exception.

Chaque compteur de statistiques de sécurité est associé à un événement de sécurité spécifique. Chaque fois qu'une statistique de sécurité est incrémentée, il convient que l'événement de sécurité correspondant soit annoncé comme cela est décrit en 7.5.3.

La mise en œuvre de tous les compteurs de statistiques de sécurité énumérés dans le Tableau 7 est obligatoire.

Pour chaque statistique de sécurité, le Tableau 7 indique le moyen mnémotechnique du journal d'événements de sécurité correspondant et l'objet de surveillance de gestion de réseaux et de systèmes (NSM - *Network and System Management*) tels qu'ils sont définis respectivement dans l'IEC 62351-14 et dans l'IEC 62351-7. L'Annexe A fournit une mise en correspondance des événements définis dans le présent document avec le concept défini dans l'IEC 62351-14.

Si l'IEC 62351-14 est mise en œuvre, les événements décrits dans le Tableau 7 doivent s'appliquer. Si l'IEC 62351-7 est mise en œuvre, l'objet de surveillance décrit dans le Tableau 7 doit s'appliquer. L'apparition de chaque événement est décrite dans le diagramme d'état correspondant de chaque procédure.

Tableau 7 – Statistiques de sécurité et événements associés

Compteur de Statistiques de Sécurité	Incrémenter chaque fois que...	Type de poste	Événement d'enregistrement	Objet de surveillance
Associations de Poste Réussies	La procédure d'Association de Poste a été réalisée avec succès.	Poste de conduite et poste téléconduit	STAS_PROC_SUCC *Notification: Réalisation réussie de l'Association de Poste*	StAsProcScsCnt *Nombre de fois que la procédure d'Association de Poste a été réalisée avec succès*
Échecs d'Association de Poste	La procédure d'Association de Poste a échoué	Poste de conduite et poste téléconduit	STAS_PROC_FAIL *Alarme: L'Association de Poste a échoué*	StAsProcFailCnt *Nombre de fois que la procédure d'Association de Poste a échoué*
Modifications réussies de Clé de Session	La procédure de Modification de Clé de Session a été réalisée avec succès	Poste de conduite et poste téléconduit	SKEY_PROC_SUCC *Notification: Réalisation réussie de Modification de Clé de Session*	SKeyProcScsCnt *Nombre de fois que la Clé de Session a été modifiée avec succès*
Échecs de Modification de Clé de Session	La procédure de Modification de Clé de Session a échoué	Poste de conduite et poste téléconduit	SKEY_PROC_FAIL *Alarme: La Modification de Clé de Session a échoué*	SKeyProcFailCnt *Nombre d'échecs de Modification de Clé de Session*
Invalidations de la Clé de Session du fait de l'expiration du Temps maximal d'Utilisation de Clé de Session	Pendant les Opérations Normales de Sécurité, les Clés de Session ont été invalidées parce que le poste de conduite ne les a pas modifiées dans l'Intervalle de Temps maximal d'Utilisation de Clé de Session.	Poste téléconduit	SKEY_INV_USETOUT *Alarme: Clé de Session invalidée du fait de la Temporisation maximale d'Utilisation de Clé de Session*	SKeyInvToutCnt *Nombre de fois que les Clés de Session ont été invalidées du fait de la Temporisation maximale d'Utilisation de Clé de Session*
Invalidations de Clés de Session du fait que le Compte Maximal d'Utilisation de Clé de Session a été atteint.	Pendant les Opérations Normales de Sécurité, les Clés de Session ont été invalidées parce que le poste de conduite ne les a pas modifiées avant d'atteindre le seuil du Compte Maximal d'Utilisation de Clé de Session.	Poste téléconduit	SKEY_INV_USECNT *Alarme: Clé de Session invalidée du fait du Compte Maximal d'Utilisation de Clé de Session*	SKeyInvUseCnt *Nombre de fois que la Clé de Session a été invalidée du fait du Compte maximal d'Utilisation de Clé de Session*
Erreurs d'Information de Protocole	Pendant la procédure d'Association de Poste, ou la procédure de Modification de Clé de Session, la valeur d'Information de Protocole fournie par le poste de conduite n'est pas admise ou n'est pas prise en charge.	Poste téléconduit	PROT_INFO_ERR *Alarme: Information de protocole non valide*	ProtInfoErrCnt *Nombre d'erreurs d'information de protocole*

Compteur de Statistiques de Sécurité	Incrémenter chaque fois que...	Type de poste	Événement d'enregistrement	Objet de surveillance
Échecs de Prise en charge de l'Algorithme d'Authentification de Clés	Pendant la procédure d'Association de Poste, l'algorithme sélectionné d'authentification de clés n'est pas admis ou n'est pas pris en charge.	Poste téléconduit	KEY_AUTNALG_SUP *Alarme: Algorithme d'authentification de clés non pris en charge*	KeyAutnAlgSupFailCnt *Nombre d'échecs de Prise en charge de l'algorithme d'authentification de clés*
Échecs de Prise en charge de l'Algorithme d'Enveloppement de Clés	Pendant la procédure d'Association de Poste, l'algorithme sélectionné d'enveloppement de clés n'est pas admis ou n'est pas pris en charge.	Poste téléconduit	KEY_WRAPALG _SUP *Alarme: Algorithme d'enveloppement de clés non pris en charge*	SKeyWrapAlgSupFailCnt *Nombre d'échecs de Prise en charge de l'algorithme d'enveloppement de clés*
Échecs de Prise en charge de l'Algorithme de Protection des Données	Pendant la procédure de Modification de Clé de Session, l'algorithme sélectionné de protection des données n'est pas admis ou n'est pas pris en charge.	Poste téléconduit	DATA_PROTALG_SUP *Alarme: Algorithme de MAC/AEAD de données non pris en charge*	DataProtAlgSupFailCnt *Nombre d'échecs de prise en charge de l'algorithme d'authentification des données*
Erreurs d'Authentification des Clés	Pendant la procédure d'Association de Poste ou la procédure de Modification de Clé de Session, l'autre poste a fourni des informations d'authentification de clés non valides.	Poste de conduite et poste téléconduit	KEY_AUTN_ERR *Alarme: Erreur d'authentification des clés*	SKeyAutnErrCnt *Nombre d'erreurs d'authentification des clés*
Erreurs d'Authentification des Données	Lors de l'Échange de Données Sécurisées, le poste local a reçu un message de Données Sécurisées non authentique.	Poste de conduite et poste téléconduit	DATA_AUTN_ERR *Avertissement: Erreur d'authentification des données*	DataAutnErrCnt *Nombre de messages de Données Sécurisées non authentiques reçus*
Messages inattendus	Le poste a reçu un message non attendu dans l'état actuel du diagramme d'état.	Poste de conduite et poste téléconduit	UNXP_MSG_ERR *Avertissement: Erreur de message inattendu*	UnxpMsgErrCnt *Nombre de messages inattendus reçus*
Nombre Maximal de Temporisations de Réponses (Voir 7.5.2)	Pendant la procédure d'Association de Poste ou la procédure de Modification de Clé de Session, le seuil du nombre Maximal de Temporisations de Réponses a été atteint.	Poste de conduite	MAX_REPLY_TOUT *Avertissement: Nombre maximal atteint de temporisations de réponses*	MaxReplyToutCnt *Nombre de fois que le seuil du nombre Maximal de Temporisations de Réponses a été atteint*
Échecs d'Autorisation du poste distant.	Pendant la procédure d'Association de Poste, le poste local reçoit un certificat de poste distant d'un poste non autorisé à communiquer.	Poste de conduite et poste téléconduit	NODE_NOT_AUTR *Alarme: Poste distant non autorisé*	NodeAutrFailCnt *Nombre de tentatives de communication non autorisées*
Échecs d'Autorisation d'Opération (Voir la Note 2)	Lors de l'Échange de Données Sécurisées, le poste téléconduit a reçu un message authentique de Données Sécurisées, mais le poste de conduite n'est pas autorisé (n'a pas le rôle/l'autorisation) à effectuer l'opération demandée.	Poste téléconduit	OPER_NOT_AUTR *Avertissement: Opération demandée non autorisée*	CtrlOperAutrFailCnt *Nombre d'opérations non autorisées*

Compteur de Statistiques de Sécurité	Incrémenter chaque fois que...	Type de poste	Événement d'enregistrement	Objet de surveillance
Échecs de vérification de Validité du Certificat du Poste Distant.	Pendant la procédure d'Association de Poste, le poste local reçoit un certificat expiré ou révoqué, voire un certificat qui contient des paramètres non valides ou une signature non valide du poste distant	Poste de conduite et poste téléconduit	REM_CERT_NOTVALID *Alarme: Certificat du poste distant non valide*	RemCertCheckFailCnt *Nombre de certificats non valides reçus*
Expirations du Certificat du Poste Distant.	Le certificat du poste distant a expiré à l'établissement de l'Association de Poste.	Poste de conduite et poste téléconduit	REM_CERT_EXPIRED Avertissement: *Expiration du Certificat du Poste Distant.*	RemCertExpiredCnt *Nombre de fois que le certificat du Poste Distant a expiré.*
Révocations du Certificat du Poste Distant. (Voir la Note 1)	Le certificat du poste distant a été révoqué par l'Autorité Centrale à l'établissement de l'Association de Poste.	Poste de conduite et poste téléconduit	REM_CERT_REVOKED Alarme: *Révocation du Certificat du Poste Distant.*	RemCertRevokedCnt *Nombre de fois que le certificat du Poste Distant a été révoqué.*
Expirations du Certificat du Poste Local.	Le certificat du poste local a expiré à l'établissement de l'Association de Poste.	Poste de conduite et poste téléconduit	LOC_CERT_EXPIRED Avertissement: *Expiration du Certificat du Poste Local.*	LocCertExpiredCnt *Nombre de fois que le certificat du poste local a expiré.*
Révocations du Certificat du Poste Local. (Voir la Note 1)	Le certificat du poste local a été révoqué par l'Autorité Centrale à l'établissement de l'Association de Poste.	Poste de conduite et poste téléconduit	LOC_CERT_REVOKED Alarme: *Révocation du certificat du poste local.*	LocCertRevokedCnt *Nombre de fois que le certificat du poste local a été révoqué.*
Invalidations des Clés Cryptographiques en raison de la Révocation du Certificat du Poste Distant. (Voir la Note 1)	Les clés cryptographiques (Clés de Mise à Jour et Clés de Session) ont été marquées comme non valides du fait de la révocation du certificat du poste distant par l'Autorité Centrale.	Poste de conduite et poste téléconduit	KEYS_INV_REMCERTREV Alarme: *Invalidations des Clés Cryptographiques en raison de la révocation du certificat du poste distant.*	KeysInvRemCertRevCnt *Nombre de fois que les Clés Cryptographiques ont été invalidées en raison de la révocation du certificat du poste distant.*
Invalidations des Clés Cryptographiques en raison de la Révocation du Certificat du Poste Local. (Voir la Note 1)	Les clés cryptographiques (Clés de Mise à Jour et Clés de Session) ont été marquées comme non valides du fait de la révocation du certificat du poste local par l'Autorité Centrale.	Poste de conduite et poste téléconduit	KEYS_INV_LOCCERTREV Alarme: *Invalidations des Clés Cryptographiques en raison de la révocation du certificat du poste local.*	KeysInvLocCertRevCnt *Nombre de fois que les Clés Cryptographiques ont été invalidées en raison de la révocation du certificat du poste local.*
Authentifications de Données réussies	Pendant les Opérations Normales Sécurisées, le poste local a reçu un message de Données Sécurisées authentique.	Poste de conduite et poste téléconduit	Aucun.	DataAutnScsCnt *Nombre de messages de Données Sécurisées authentiques reçus*
Temporisations de réponse	Pendant la procédure d'Association de Poste ou la procédure de Modification de Clé de Session, le poste téléconduit n'a pas répondu dans le délai de Temps de Réponse Prévu.	Poste de conduite	Aucun.	ReplyToutCnt *Nombre de Temporisations de Réponse*
Temporisations de requête	Pendant la procédure d'Association de Poste ou la procédure de Modification de Clé de Session, le poste de conduite n'a pas envoyé de requête dans le délai de Temps de Réponse Prévu.	Poste téléconduit	Aucun.	RequestToutCnt *Nombre de Temporisations de Requête*

Compteur de Statistiques de Sécurité	Incrémenter chaque fois que...	Type de poste	Événement d'enregistrement	Objet de surveillance
Nombre Total de Messages Envoyés	Le poste envoie une ASDU	Poste de conduite et poste téléconduit	Aucun.	TxPduCnt. *Nombre de PDU transmises*
Nombre Total de Messages Reçus	Le poste reçoit une ASDU	Poste de conduite et poste téléconduit	Aucun.	RxPduCnt. *Nombre de PDU reçues (y compris les PDU comprenant des erreurs)*
Messages ignorés	Le poste ignore un message reçu.	Poste de conduite et poste téléconduit	Aucun.	DiscPduCnt *Nombre de messages ignorés*
NOTE 1 Cette statistique de sécurité est applicable si l'Autorité Centrale est prise en charge. Voir 8.3.9. NOTE 2 Cette statistique de sécurité est applicable si l'Autorité Centrale et le Contrôle d'Accès Basé sur les Rôles (RBAC - *Role Base Access Control*) sont pris en charge. Voir 8.5.6.1.				

7.5.2 Seuils de sécurité spéciaux

De plus, les diagrammes d'états doivent utiliser le seuil mobile suivant afin de déterminer quand réagir aux conditions d'erreur, comme cela est spécifié dans les procédures formelles décrites à l'Article 8:

- Nombre Maximal de Temporisations de Réponses (poste de conduite uniquement): Nombre maximal de temporisations de réponses admises dans une session qui attend une réponse spécifique du poste téléconduit.

Si ce seuil est atteint, l'événement doit entraîner le dispositif à réaliser des actions spécifiques – autres que la simple consignation de l'événement – comme cela est décrit dans le diagramme d'état.

Chaque fois que le diagramme d'état "réinitialise" la valeur du nombre Maximal de Temporisations de Réponses, il doit ajouter le seuil configuré pour cette statistique à la valeur en cours du nombre Maximal de Temporisations de Réponses. Le poste de conduite doit réinitialiser toutes les valeurs du nombre Maximal de Temporisations de toutes Associations au démarrage.

7.5.3 Rapport des statistiques de sécurité

Les dispositifs doivent permettre l'accès aux statistiques de sécurité sans modification ou qu'elles fassent l'objet d'un rapport en utilisant les services de protocole concernés ou par d'autres moyens.

De plus, le poste téléconduit doit être capable de consigner ces compteurs de statistiques de sécurité au poste de conduite en utilisant les méthodes appropriées pour le protocole concerné.

La méthode employée pour transmettre les statistiques de sécurité au moyen du protocole concerné doit être définie dans les normes de référence du protocole concerné.

Chaque poste doit permettre la configuration d'un seuil pour chacune des statistiques de sécurité énumérées dans le Tableau 7. Le poste téléconduit doit transmettre la valeur de la statistique de sécurité au poste de conduite chaque fois que la valeur de seuil correspondante est atteinte.

Chaque fois que le poste téléconduit transmet une valeur de statistique, il doit "réinitialiser" le seuil correspondant à la valeur en cours de la statistique augmentée de la valeur configurée pour ce seuil. Les dispositifs doivent réinitialiser toutes les valeurs de seuil au démarrage.

La valeur par défaut des seuils de statistiques de sécurité doit être définie dans les normes de référence du protocole concerné.

7.5.4 Surveillance et enregistrement des événements de sécurité

Les événements du présent mécanisme de communication sécurisée, décrits dans le Tableau 7, sont définis comme des avertissements et alarmes. Ces événements de sécurité sont destinés à prendre en charge la gestion des erreurs et à augmenter ainsi la résilience d'un système. Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.

Noter que les avertissements et alarmes sont utilisés pour indiquer la sévérité d'un événement du point de vue de la sécurité. Il est prévu qu'une politique de sécurité de l'opérateur détermine le traitement final selon l'environnement opérationnel.

Il est recommandé de mettre en œuvre les événements de sécurité (notifications, avertissements et alarmes) de l'ensemble du document en surveillant les objets comme cela est spécifié par l'IEC 62351-7 et/ou par événements d'enregistrement comme cela est spécifié par l'IEC 62351-14. L'IEC 62351-7 définit la gestion des informations relatives à la surveillance de sécurité, tandis que l'IEC 62351-14 spécifie la gestion des messages d'avertissement de sécurité et d'alarme de sécurité.

Des méthodes alternatives de surveillance et d'enregistrement de sécurité peuvent être spécifiées dans les normes de référence du protocole concerné.

Il est fortement recommandé d'enregistrer les avertissements et alarmes de sécurité de l'ensemble du document sur des dispositifs locaux. La méthode d'enregistrement locale, le nombre de journaux et la durée pendant laquelle les journaux doivent être conservés constituent un problème de mise en œuvre local et ne relèvent pas du domaine d'application du présent document.

8 Procédures formelles

8.1 Vue d'ensemble du paragraphe

L'Article 8 décrit de manière formelle et en détail les procédures du protocole de sécurité, les messages et les données échangés.

Les dispositifs revendiquant la conformité à la présente norme doivent mettre en œuvre le mécanisme de communication sécurisé décrit à l'article 8 indépendamment pour chaque association entre une station de contrôle et une station contrôlée.

8.2 Distinction entre messages et ASDU

8.2.1 Généralités

Un message de sécurité n'est pas une ASDU complète. La liste des données et le format de ces données doivent rester les mêmes entre les protocoles, mais les ASDU qui entourent le message et les mécanismes qui servent à les remettre doivent être différents d'un protocole à l'autre. Cette mise en correspondance avec le protocole concerné doit être décrite dans les normes de référence du protocole concerné, comme cela est examiné à l'Article 10. Noter que l'ensemble des protocoles concernés transmet des valeurs entières dont l'octet le moins significatif est transmis en premier. La même convention doit donc être utilisée pour l'ensemble des messages de sécurité.

8.2.2 Types des données et notations des messages

Les types des données utilisés dans le présent document, dans les paragraphes de Définition des Données, sont définis dans l'IEC 60870-5-4.

8.3 Procédure d'Association de Poste

8.3.1 Généralités

La procédure d'Association de Poste est réalisée pour établir une association entre le poste de conduite et le poste téléconduit, pour identifier la liaison de communication entre les deux postes, le Rôle du poste de conduite et pour générer les Clés de Mise à Jour associées. Chaque dispositif doit maintenir un ensemble unique de Clés de Mise à Jour pour chacune des associations établies.

Cette procédure est réalisée pendant la mise en service (installation du poste de conduite et/ou du poste téléconduit) ou lorsque cela est demandé par l'Autorité Centrale chaque fois qu'un nouveau certificat est fourni au poste de conduite ou au poste téléconduit.

En fonction de la politique de sécurité de l'organisation, l'Autorité Centrale ou le personnel autorisé peut également exiger que le poste de conduite initie la procédure d'Association de Poste, même de manière régulière pour un renouvellement périodique des Clés de Mise à Jour. La méthode utilisée pour demander au poste de conduite d'initier la procédure d'Association de Poste ne relève pas du domaine d'application du présent document.

Des conditions supplémentaires d'initialisation de la procédure d'Association de Poste peuvent être spécifiées dans les normes de référence du protocole concerné.

Cette procédure met en œuvre l'échange des mécanismes Diffie-Hellmann basés sur une courbe elliptique (ECDH) qui utilise des certificats de clés publiques et une Fonction de Dérivation de Clé fondée sur le Hachage (HKDF) sur les informations échangées pour générer les Clés de Mise à Jour (conformément aux documents RFC 5869 et RFC 7748).

8.3.2 Certificats de clés publiques

8.3.2.1 Généralités

La procédure d'Association de Poste exige l'utilisation de certificats de clés publiques (certificats de dispositifs). Les certificats de dispositif doivent être un certificat X.509 et la clé publique doit être une clé ECDH. La longueur minimale de la clé publique de dispositif doit être de 256 bits.

Les certificats de dispositif peuvent être soit autosignés par le dispositif, soit signés par l'Autorité Centrale si cette dernière est prise en charge (facultatif).

Le poste téléconduit doit pouvoir identifier de manière unique chaque poste de conduite qui communique vers lui. Ce mécanisme de sécurité exige donc que la valeur *Distinguished Name (DN)* dans les certificats de dispositif soit unique pour chaque dispositif de l'organisation.

Les mises en œuvre dont la conformité au présent document est revendiquée doivent être capables de prendre en charge un certificat de clé publique de 8192 octets ou moins. La taille des certificats de clés publiques dépend de la politique de sécurité de l'organisation.

Les mises en œuvre qui revendiquent la conformité au présent document doivent être capables de prendre en charge l'échange de certificats X.509 au format des règles de codage identifiées (DER - *Distinguished Encoding Rule*). Pendant la procédure d'Association de Poste, les certificats X.509 doivent être transmis au format DER.

8.3.2.2 Courbes cryptographiques

Le Tableau 8 énumère les Courbes Elliptiques, dont la prise en charge est obligatoire ou facultative, utilisées pour générer la paire de clés publique/privée et pour signer les certificats X.509. Des courbes supplémentaires peuvent être spécifiées dans les normes de référence du protocole concerné.

Tableau 8 – Courbes cryptographiques elliptiques

Courbe EC	Spécifiée dans le document	Prise en charge obligatoire ou facultative (o/f)
Courbe 25519	RFC 7748	o
Courbe 448	RFC 7748	o
secp256k1	SEC2-V2	o
secp256r1	SEC2-V2	o
brainpoolP256r1	RFC 5639	f

Le document RFC 7748 spécifie l'ensemble des paramètres de génération de chaque courbe, ainsi que le point de la courbe utilisé pour générer les clés publiques et privées.

La paire de clés publique/privée de dispositif dans les dispositifs autorisés à communiquer doit être générée à l'aide de la même courbe. Par conséquent, les certificats de courbe EC de dispositif échangés au cours de la procédure d'Association de Poste doivent spécifier la même courbe EC.

Noter que la prise en charge de la Courbe 25519 et de la Courbe 448 n'est prévue que dans le contexte d'un agrément de clé ECDH, et pas dans le contexte de signatures numériques.

Dans le cas d'une signature numérique de certificats X.509, la courbe EC utilisée doit être: secp256k1 ou secp256r1. En option, brainpoolP256r1 peut être pris en charge.

8.3.2.3 Utilisation de certificats autosignés

Les dispositifs dont la conformité à la présente norme est revendiquée doivent prendre en charge les certificats autosignés de clés publiques.

Si des certificats autosignés sont utilisés, la clé publique du certificate, ou l'empreinte digitale du certificate du poste distant, reçue pendant la procédure d'Association de Poste, doit être préfournie à chaque dispositif.

Les certificats autosignés des dispositifs doivent être signés avec la clé privée de dispositif au moyen de l'algorithme de signature numérique de courbe elliptique (ECDSA - *Elliptic Curve Digital Signature Algorithm*) associé à l'algorithme de hachage sécurisé SHA-256 tel qu'il est défini dans le document Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA) [X9.62].

La courbe EC utilisée dans ce mécanisme de communication sécurisée pour signer les certificats autosignés doit être Secp256k1 ou Secp256r1 définie dans le document SEC2-V2: Recommended Elliptic Curve Domain Parameters – Version 2.0. De manière facultative, la courbe EC brainpoolP256r1 définie dans le document RFC 5639 peut être utilisée si elle est prise en charge.

Dans ce mécanisme de communication sécurisée, les certificats autosignés ne doivent pas contenir d'informations RBAC.

8.3.2.4 Utilisation de certificats signés par l'Autorité Centrale

Si l'Autorité Centrale est prise en charge, les certificats de dispositifs signés par l'Autorité Centrale peuvent être utilisés dans la procédure d'Association de Poste. L'Autorité Centrale devient dans ce cas l'Autorité de Certification émettrice.

Les certificats signés par l'Autorité Centrale peuvent être soit des certificats signés avec la clé ECDSA, soit des certificats signés avec la clé RSA. Si l'Autorité Centrale est prise en charge, les dispositifs doivent prendre en charge les certificats signés avec la clé ECDSA ou la clé RSA. L'algorithme de hachage utilisé dans la création de la signature des certificats ECDSA ou RSA doit être au moins SHA-256.

Pour les certificats signés avec la clé ECDSA, la longueur de clé minimale doit être de 256 bits, et pour les certificats signés avec la clé RSA, la longueur de clé minimale doit être de 2048 bits.

Si les certificats signés avec la clé ECDSA sont utilisés, la courbe EC utilisée dans ce mécanisme de communication sécurisée pour signer les certificats de clés publiques doit être Secp256k1 ou Secp256r1 définie dans le document SEC2-V2: Recommended Elliptic Curve Domain Parameters – Version 2.0. De manière facultative, la courbe EC brainpoolP256r1 définie dans le document RFC 5639 peut être utilisée si elle est prise en charge.

L'utilisation des certificats de clé publique n'est admise que conjointement au certificat de clé publique de l'Autorité Centrale correspondant. Si le certificat de clé publique de l'Autorité Centrale n'est pas disponible au niveau du poste local, le certificat de clé publique du poste distant ne doit pas être accepté par le poste local.

Dans ce mécanisme de communication sécurisée, les certificats signés par l'Autorité Centrale peuvent contenir d'informations relatives au RBAC. Pour la prise en charge du RBAC dans les certificats de clés publiques, le Profil A de l'IEC 62351-8 doit être pris en charge.

8.3.2.5 Utilisation de certificats d'attribut

Si l'Autorité Centrale est prise en charge, le poste de conduite peut fournir un certificat d'attribut (décrit dans le document RFC 5755) au poste téléconduit au lieu du certificat de clé publique (par exemple, pour modifier les informations relatives au RBAC) si le certificat de clé publique du dispositif correspondant a déjà été fourni au poste téléconduit dans une procédure d'Association de Poste réalisée avec succès auparavant, ou par d'autres moyens.

L'utilisation d'un certificat d'attribut n'est admise que conjointement au certificat de clé publique de l'Autorité Centrale correspondant. Si le certificat de clé publique de l'Autorité Centrale n'est pas disponible au niveau du poste téléconduit, le certificat d'attribut ne doit pas être accepté par le poste téléconduit.

Par ailleurs, l'utilisation d'un certificat d'attribut n'est admise que conjointement au certificat de clé publique du poste de conduite correspondant, signé par l'Autorité Centrale. Si le certificat de clé publique du poste de conduite n'est pas disponible au niveau du poste téléconduit, le certificat d'attribut ne doit pas être accepté par le poste téléconduit.

Noter que l'utilisation des certificats d'attribut entre le poste de conduite et le poste téléconduit peut prendre en charge des cas d'utilisation dans lesquels deux entités juridiques accèdent au composant de sous-poste avec des rôles différents.

Pour la prise en charge du RBAC qui utilise des certificats d'attribut, le Profil B de l'IEC 62351-8 doit être pris en charge.

8.3.3 Configuration des postes distants autorisés

Les dispositifs doivent permettre à un utilisateur de configurer une liste des clés publiques des postes distants autorisés à communiquer avec le poste local. Cette exigence permet à l'organisation d'utiliser des certificats autosignés si l'autorité centrale n'est pas prise en charge. Cette configuration ne doit être permise qu'au personnel autorisé. La méthode d'identification et de configuration des postes distants autorisés sur les dispositifs ne relève pas du domaine d'application de la présente norme. Noter qu'il convient d'identifier un poste distant sur la base d'identifiants uniques dans le domaine de l'opérateur.

8.3.4 Conditions préalables pour initier la procédure d'Association de Poste

Avant d'initier la procédure d'Association de Poste (par exemple, pendant l'installation du dispositif), les éléments suivants doivent être fournis à chaque dispositif:

a) le certificat de dispositif X.509;

b) si les dispositifs génèrent des certificats autosignés (ou en sont fournis):

- la clé publique, ou empreinte digitale du certificate, du poste distant correspondante doit être fournie aux dispositifs.

  Si les dispositifs sont fournis en certificats signés par l'Autorité Centrale:

- le certificat X.509 de l'Autorité Centrale qui délivre le certificat du poste téléconduit doit être fourni au poste de conduite;
- le certificat X.509 de l'Autorité Centrale qui délivre le certificat du poste de conduite doit être fourni au poste téléconduit.

Si un certificat X.509 valide n'est pas fourni au dispositif, le mécanisme de sécurité entier décrit dans la présente norme ne peut pas être exécuté.

La fourniture des certificats de clés publiques et de la clé publique du poste distant sur les dispositifs ne doit être permise qu'à l'Autorité Centrale ou au personnel autorisé. La méthode de fourniture des certificats de clés publiques et de la clé publique du poste distant sur les dispositifs ne relève pas du domaine d'application de la présente norme.

Si la fourniture de certificats de clés publiques aux dispositifs est automatisée, il convient qu'elle respecte l'un des mécanismes décrits dans l'IEC 62351-9.

8.3.5 Définition des messages

8.3.5.1 Généralités

Le paragraphe 8.3.5 décrit les messages de sécurité et les données échangées dans chaque message de sécurité qui exécute la procédure d'Association de Poste. La Figure 3 représente en détail les messages et les données échangés.

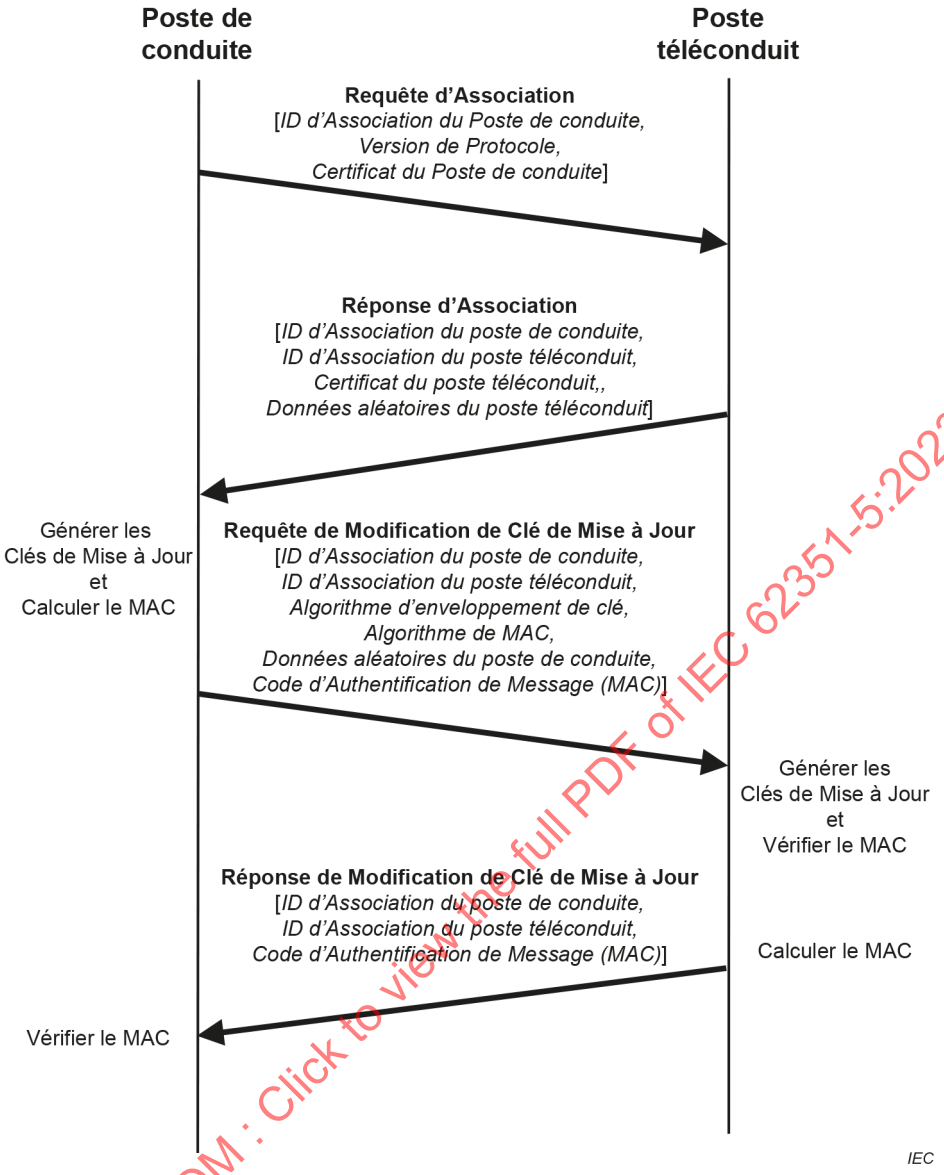


Figure 3 – Procédure d'Association de Poste

8.3.5.2 Message de Requête d'Association

8.3.5.2.1 Structure

Chaque message de Requête d'Association doit contenir les informations décrites en 8.3.5.2 et résumées dans le Tableau 9.

Seul le poste de conduite doit envoyer le message de Requête d'Association. Le message de Requête d'Association doit entraîner un message de Réponse d'Association de la part du poste téléconduit.

Après l'envoi du message de Requête d'Association, le poste de conduite doit enclencher l'Horloge de Réponse afin de vérifier que le message de Réponse d'Association du poste téléconduit est reçu dans le délai prévu. Si l'Horloge de Réponse expire (Temporisation de Réponse), le poste de conduite doit exécuter les actions indiquées dans le diagramme d'état correspondant décrit en 8.3.6.

Tableau 9 – Message de Requête d'Association

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur Valeur	PRI = Information de protocole
Valeur Valeur	CDL = Longueur de données du certificat du poste de conduite
Nombre d'octets spécifié dans la CDL	CDC = Données du certificat du poste de conduite

8.3.5.2.2 ID d'Association du Poste de Conduite

Il s'agit de la valeur que le poste de conduite a choisie pour représenter la liaison de communication avec ce poste téléconduit. Sur le poste de conduite, cette valeur doit être unique pour chaque association avec les postes téléconduits. Les normes de référence du protocole concerné peuvent exiger des valeurs d'AIM spécifiques dans ce message.

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

8.3.5.2.3 ID d'Association du Poste Téléconduit

Cette valeur est de 0 (zéro) par défaut dans ce message. Les normes de référence du protocole concerné peuvent exiger des valeurs d'AIS spécifiques dans ce message.

AIS:= UI16[1..16]<0>

8.3.5.2.4 Information de Protocole

Le poste de conduite utilise ce champ pour fournir l'information de protocole, y compris la version de protocole qu'il a l'intention d'utiliser avec le poste téléconduit.

La structure et les valeurs possibles dans ce champ doivent être spécifiées par les normes de référence du protocole concerné.

Le poste de conduite et le poste téléconduit peuvent prendre en charge de multiples versions de protocole. Le poste téléconduit doit valider la valeur d'Information de Protocole spécifiée dans le message de Requête d'Association reçu. Les règles de validation de la valeur d'Information de Protocole sur le poste téléconduit doivent être spécifiées dans les normes de référence du protocole concerné. Si la valeur d'Information de Protocole est considérée comme non valide dans la norme de référence, le poste téléconduit doit ignorer la Requête de Session reçue.

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

8.3.5.2.5 Longueur de Données du Certificat du Poste de Conduite

Le poste de conduite doit utiliser ce champ pour spécifier la longueur des données du Certificat X.509 du Poste de Conduite qui suit.

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

8.3.5.2.6 Données du Certificat du Poste de Conduite

Le poste de conduite doit utiliser ce champ pour fournir le certificat X.509 ECDSA au poste téléconduit.

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

8.3.5.3 Message de Réponse d'Association

8.3.5.3.1 Structure

Chaque message de Réponse d'Association doit contenir les informations décrites en 8.3.5.3 et résumées dans le Tableau 10.

Le poste téléconduit (seulement) doit envoyer le message de Réponse d'Association chaque fois qu'un message de Requête d'Association valide est reçu du poste de conduite.

Le message de Réponse d'Association fournit le certificat du poste téléconduit et les données aléatoires associées au poste de conduite. Le poste de conduite doit utiliser ces informations pour authentifier le message de Requête de Modification de Clé de Mise à Jour qui suit.

Après l'envoi du message de Réponse d'Association, le poste téléconduit doit enclencher l'Horloge de Requête afin de vérifier que le message de Requête de Modification de Clé de Mise à Jour du poste de conduite qui suit est reçu dans le délai prévu. Si l'Horloge de Requête expire (Temporisation de Requête), le poste téléconduit doit exécuter les actions indiquées dans le diagramme d'état correspondant décrit en 8.3.7.

L'Horloge de Réponse doit être arrêtée lorsqu'un message de Requête de Modification de Clé de Mise à Jour valide est reçu.

Tableau 10 – Message de Réponse d'Association

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur Valeur	CDL = Longueur de données du certificat du poste téléconduit
Valeur	CGL = Longueur de données aléatoires du poste téléconduit
Nombre d'octets spécifiés dans la CDL	CDC = Données du certificat du poste téléconduit
Nombre d'octets spécifiés dans la CGL	CGD = Données aléatoires du poste téléconduit

8.3.5.3.2 ID d'Association du Poste de Conduite

Cette valeur doit correspondre à l'AIM dans le message de Requête d'Association reçu le plus récemment du poste de conduite, décrit en 8.3.5.2.

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

8.3.5.3.3 ID d'Association du Poste Téléconduit

Il s'agit de la valeur que le poste téléconduit a choisie pour représenter la liaison de communication avec ce poste de conduite. Sur le poste téléconduit, cette valeur doit être unique pour chaque association établie avec les postes de conduite. Les normes de référence du protocole concerné peuvent exiger des valeurs d'AIS spécifiques dans ce message.

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

8.3.5.3.4 Longueur de Données du Certificat du Poste Téléconduit

Le poste téléconduit doit utiliser ce champ pour spécifier la longueur des données du certificat de dispositif X.509 du poste téléconduit qui suit.

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

8.3.5.3.5 Longueur de Données Aléatoires du Poste Téléconduit

Cette valeur doit spécifier la longueur en octets des données aléatoires qui suivent. La longueur minimale des données aléatoires dans ce message doit être de quatre octets, la longueur maximale est de 64 octets.

CGL:= UI8[1..8]<4 ..64>

8.3.5.3.6 Données du Certificat du Poste Téléconduit

Le poste téléconduit doit utiliser ce champ pour fournir le certificat X.509 au poste de conduite.

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

8.3.5.3.7 Données Aléatoires du Poste Téléconduit

Le poste téléconduit doit inclure ces données aléatoires dans le message de Réponse d'Association afin d'assurer que le contenu du message de Requête de Modification de Clé de Mise à Jour qui suit n'est pas prévisible. Ces données aléatoires sont également utilisées pour dériver les Clés de Mise à Jour, comme cela est décrit en 8.3.10. Les générateurs de nombres aléatoires sont chargés de fournir des données aléatoires statistiquement adéquates. Des conseils pour la génération de nombres aléatoires peuvent être trouvés dans NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C ainsi que dans IETF RFC 4086.

CGD:= OS8i[1..8i]; i:=CGL

8.3.5.4 Message de Requête de Modification de Clé de Mise à Jour

8.3.5.4.1 Structure

Chaque message de Requête de Modification de Clé de Mise à Jour doit contenir les informations décrites en 8.3.5.4 et résumées dans le Tableau 11.

Seul le poste de conduite doit envoyer des messages de Requête de Modification de Clé de Mise à Jour. Le message de Requête de Modification de Clé de Mise à Jour fournit des informations utilisées par le Poste Téléconduit pour calculer et vérifier les Clés de Mise à Jour.

Après l'envoi du message de Requête de Modification de Clé de Mise à Jour, le poste de conduite doit enclencher l'Horloge de Réponse afin de vérifier que le message de Réponse de Modification de Clé de Mise à Jour du poste téléconduit est reçu dans le délai prévu. Si l'Horloge de Réponse expire (Temporisation de Réponse), le poste de conduite doit exécuter les actions indiquées dans le diagramme d'état décrit en 8.3.6.

Tableau 11 – Message de Requête de Modification de Clé de Mise à Jour

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur énumérée	KWA = Algorithme d'enveloppement de Clé de Session
Valeur énumérée	MAL = algorithme de MAC
Valeur	CGL = Longueur de données aléatoires du poste de conduite
Nombre d'octets spécifié dans la CCL	CGD = Données aléatoires du poste de conduite
Nombre d'octets spécifié par l'algorithme de MAC (MAL) choisi dans ce message, défini en 8.3.5.4.5	MAC = Code d'authentification de message

8.3.5.4.2 ID d'Association du Poste de Conduite

Il s'agit de la valeur que le poste de conduite a choisie pour représenter la liaison de communication avec ce poste téléconduit. Sur le poste de conduite, cette valeur doit être unique pour chaque association avec les postes téléconduits. Cette valeur ne peut pas être 0 (zéro).

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

8.3.5.4.3 ID d'Association du Poste Téléconduit

Cette valeur doit correspondre à l'AIS dans le message de Réponse d'Association reçu le plus récemment du poste téléconduit, décrit en 8.3.5.3.

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

8.3.5.4.4 Algorithme d'Enveloppement de Clé de Session

En utilisant ce champ, le poste de conduite doit indiquer au poste téléconduit l'algorithme choisi pour chiffrer/décrypter les Clés de Session pendant la procédure de Modification de Clé de Session, décrite en 8.4.

Les algorithmes d'enveloppement de clé dont la prise en charge est obligatoire sont énumérés à l'Article 9: Exigences d'interopérabilité. Il convient de choisir la meilleure option disponible dans ce champ.

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

<0>:= pas utilisé

<1>:= devenu obsolète

<2>:= Algorithme d'Enveloppement de Clé AES-256

<3..127>:= réservé pour utilisation ultérieure

<128..255>:= réservé pour les choix spécifiques au fournisseur. Interopérabilité non garantie.

8.3.5.4.5 Algorithme de MAC

En utilisant ce champ, le poste de conduite doit indiquer au poste téléconduit l'algorithme choisi pour calculer les valeurs de MAC et leur longueur résultante dans les messages authentifiés échangés dans cette session d'authentification (Requête de Modification de Clé de Mise à Jour, Réponse de Modification de Clé de Mise à Jour), ainsi que dans les messages authentifiés échangés dans l'ensemble des procédures de Modification de Clé de Mise à Jour suivantes réalisées (Requête de Modification de Clé de Session, Réponse de Modification de Clé de Session) décrites en 8.4.

Les algorithmes de MAC dont la prise en charge est obligatoire sont énumérés à l'Article 9: Exigences d'Interopérabilité. Il convient de choisir la meilleure option disponible dans ce champ.

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

<0>:= réservé

<1>:= réservé

<2>:= devenu obsolète

<3>:= HMAC-SHA-256 tronqué à 8 octets (en série)

<4>:= HMAC-SHA-256 tronqué à 16 octets (en réseau)

<5>:= devenu obsolète

<6>:= devenu obsolète

<7>:= HMAC-SHA3-256 tronqué à 8 octets (en série)

<8>:= HMAC-SHA3-256 tronqué à 16 octets (en réseau)

<9>:= BLAKE2s-256 tronqué à 8 octets (en série)

<10>:= BLAKE2s-256 tronqué à 16 octets (en réseau)

<11..127>:= réservé pour utilisation ultérieure

<128..255>:= réservé pour les choix spécifiques au fournisseur. Interopérabilité non garantie.

8.3.5.4.6 Longueur de Données Aléatoires du Poste de Conduite

Le poste de conduite doit utiliser ce champ pour spécifier la longueur des données aléatoires qui suivent. La longueur minimale des données aléatoires doit être de quatre octets, la longueur maximale est de 64 octets.

CGL:= UI8[1..8]<4 ..64>

8.3.5.4.7 Données Aléatoires du Poste de Conduite

Le poste de conduite doit envoyer ces données pour éviter les attaques par rejeu lors de la modification des Clés de Mise à Jour. Ces données aléatoires sont également utilisées pour dériver les Clés de Mise à Jour, comme cela est décrit en 8.3.10. Les générateurs de nombres aléatoires sont chargés de fournir des données aléatoires statistiquement adéquates. Des conseils pour la génération de nombres aléatoires peuvent être trouvés dans NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C ainsi que dans IETF RFC 4086.

CGD:= OS8i[1..8i]; i:=CGL

8.3.5.4.8 Code d'Authentification de Message

Le poste de conduite doit utiliser ce champ pour authentifier les données incluses dans le message de Requête de Modification de Clé de Mise à Jour en transmission.

Cette valeur doit être calculée au moyen de l'algorithme de MAC choisi dans ce message, décrit en 8.3.5.4.5, en utilisant la **Clé de Mise à Jour d'Authentification** correspondante générée comme cela est décrit en 8.3.10.

Le poste de conduite doit faire passer les données par l'algorithme de MAC dans l'ordre décrit dans le Tableau 12, les normes de référence peuvent nécessiter des informations complémentaires, en plus de celles indiquées dans Tableau 12, à inclure dans le calcul du MAC. La longueur de la valeur de MAC résultante, en fonction de l'algorithme de MAC choisi, doit être tronquée comme cela est indiqué en 8.3.5.4.5.

Tableau 12 – Données incluses dans le calcul de MAC (dans cet ordre)

Données	Description	Décrites au	Source
Données Aléatoires du Poste Téléconduit	Les données aléatoires fournies par le poste téléconduit dans le message de Réponse d'Association reçu le plus récemment.	Paragraphe 8.3.5.3.7	Réponse d'Association
Valeurs de Requête de Modification de Clé de Mise à Jour	L'intégralité du message de Requête de Modification de Clé de Mise à Jour en transmission jusqu'au CGD compris (à l'exclusion du champ MAC).	Paragraphe 8.3.5.4	Requête de Modification de Clé de Mise à Jour
Données de remplissage	Données de remplissage supplémentaires exigées par l'algorithme de MAC.	Spécification de l'algorithme.	Exigé par l'algorithme.

MAC:= OS8i[1..8i]; i:=comme cela est spécifié dans le MAL de ce message, défini en 8.3.5.4.5.

8.3.5.5 Message de Réponse de Modification de Clé de Mise à Jour

8.3.5.5.1 Structure

Chaque message de Réponse de Modification de Clé de Mise à Jour doit contenir les informations décrites en 8.3.5.5 et résumées dans le Tableau 13.

Seul le poste téléconduit doit envoyer un message de Réponse de Modification de Clé de Mise à Jour. L'échange de ce message assure que le poste de conduite et le poste téléconduit sont en accord sur les informations suivantes:

– l'identité du poste de conduite et du poste téléconduit;

– les nouvelles Clés de Mise à Jour;

– l'ID d'Association du Poste de Conduite (AIM) que ce dernier associe à ces Clés de Mise à Jour dans toutes les authentifications suivantes;

– l'ID d'Association du Poste Téléconduit (AIS) que le poste téléconduit associe à ces Clés de Mise à Jour dans toutes les authentifications suivantes;
– le Rôle du poste de conduite sur ce poste téléconduit (si l'Autorité Centrale et le RBAC sont pris en charge).

Tableau 13 – Message de Réponse de Modification de Clé de Mise à Jour

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Nombre d'octets spécifié par l'algorithme de MAC (MAL) choisi dans la Requête de Modification de Clé de Mise à Jour valide reçue le plus récemment, définie en 8.3.5.4.5	MAC = Code d'authentification de message

8.3.5.5.2 ID d'Association du Poste de Conduite

Cette valeur doit correspondre à l'AIM dans le message de Requête de Modification de Clé de Mise à Jour reçu le plus récemment du poste de conduite, décrit en 8.3.5.4.2.

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

8.3.5.5.3 ID d'Association du Poste Téléconduit

Il s'agit de la valeur que le poste téléconduit a choisie pour représenter la liaison de communication avec ce poste de conduite. Sur le poste téléconduit, cette valeur doit être unique pour chaque association établie avec les postes de conduite. Cette valeur ne peut pas être 0 (zéro).

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

8.3.5.5.4 Code d'Authentification de Message

Le poste de conduite doit utiliser ce champ pour authentifier les données incluses dans le message de Réponse de Modification de Clé de Mise à Jour en transmission.

Cette valeur doit être calculée au moyen de l'algorithme de MAC choisi dans la Requête de Modification de Clé de Mise à Jour reçue le plus récemment, décrit en 8.3.5.4.5, en utilisant la Clé de Mise à Jour d'Authentification correspondante générée comme cela est décrit en 8.3.10.

Le poste de conduite doit faire passer les données par l'algorithme de MAC dans l'ordre décrit dans le Tableau 14. La longueur de la valeur de MAC résultante, en fonction de l'algorithme de MAC choisi, doit être tronquée comme cela est indiqué en 8.3.5.4.5.

Tableau 14 – Données incluses dans le calcul de MAC (dans cet ordre)

Données	Description	Décrites au	Source
Valeurs de Requête de Modification de Clé de Mise à Jour	L'intégralité du message de Requête de Modification de Clé de Mise à Jour reçu le plus récemment	Paragraphe 8.3.5.4	Requête de Modification de Clé de Mise à Jour
Valeurs de Réponse de Modification de Clé de Mise à Jour	L'intégralité du message de Réponse de Modification de Clé de Mise à Jour en transmission jusqu'à l'AIS compris (à l'exclusion du champ MAC).	Paragraphe 8.3.5.5	Réponse de Modification de Clé de Mise à Jour
Données de remplissage	Données de remplissage supplémentaires exigées par l'algorithme de MAC.	Spécification de l'algorithme.	Comme cela est exigé par l'algorithme.

MAC:= OS8i[1..8i]; i:=comme cela est spécifié dans le MAL du message de Requête de Modification de Clé de Mise à Jour reçu le plus récemment, défini en 8.3.6.4.5.

8.3.5.6 Procédure d'association sollicitée par le poste téléconduit

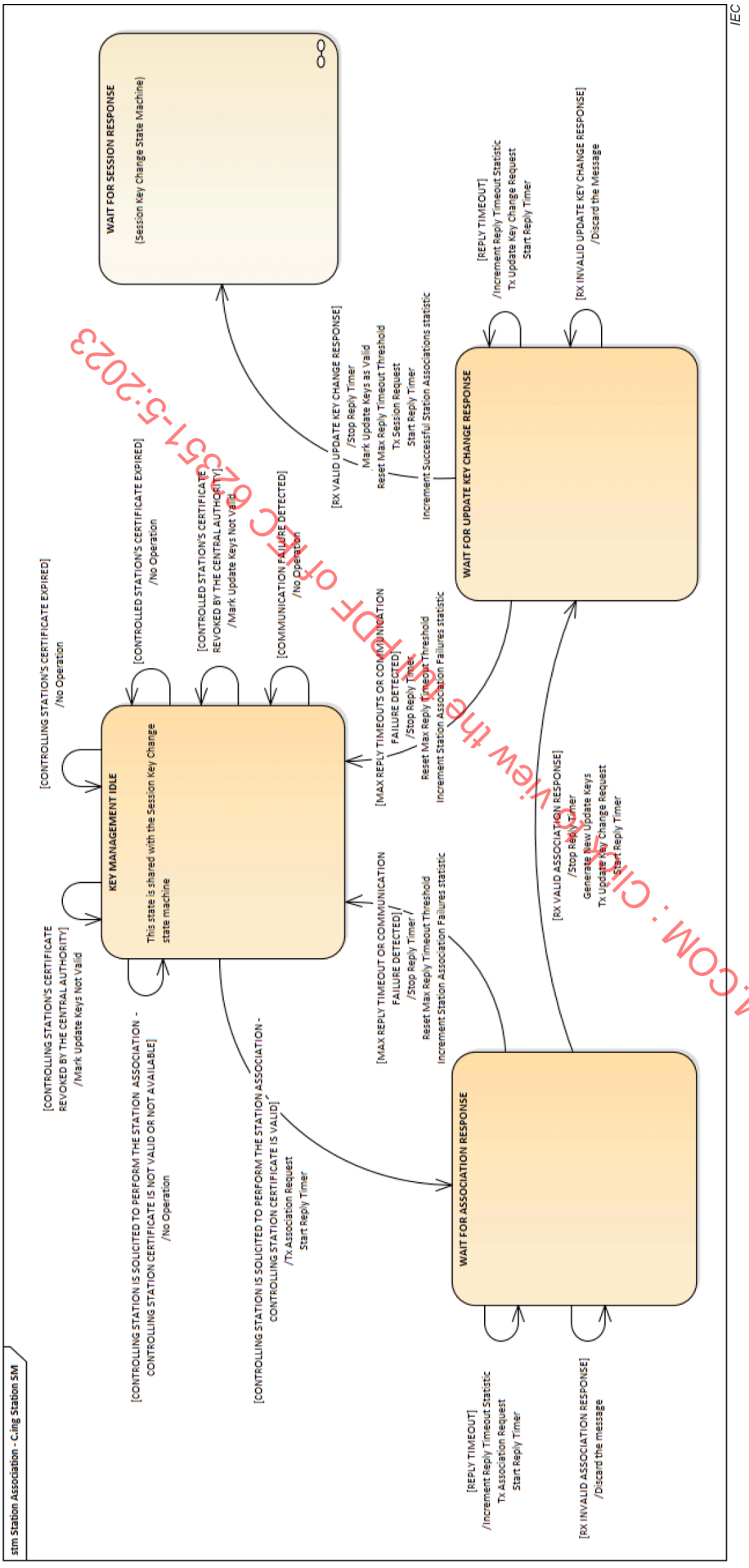
Si des messages non sollicités spontanés en provenance du poste téléconduit sont admis, ce dernier peut, de manière facultative, solliciter le poste de conduite pour qu'il initie la procédure d'Association par l'envoi d'un message de Requête d'Initiation d'Association. Les normes de référence du protocole concerné peuvent définir le message de Requête d'Initiation d'Association et sa gestion.

8.3.5.7 Prise en charge simultanée d'associations sur le poste téléconduit

Il est fortement recommandé que le poste téléconduit limite le nombre d'associations prises en charge simultanément. Le poste téléconduit est autorisé à ne pas répondre à une Requête d'Association quelconque si cette limite est dépassée.

8.3.6 Diagramme d'état du poste de conduite

Sur le poste de conduite, les messages d'Association de Poste décrits en 8.3.5 doivent être gérés par le diagramme d'état décrit en 8.3.6. La Figure 4 représente les transactions de l'Association de Poste sur le poste de conduite. Le poste de conduite doit exécuter le diagramme d'état Association de Poste décrit dans le Tableau 15. L'état *Inactif de Gestion de Clés* est partagé (en commun) avec le diagramme d'état Modification de Clé de Session.



Anglais	Français
CONTROLLING STATION'S CERTIFICATE REVOKED BY THE CENTRAL AUTHORITY/ Mark Update Keys Not Valid	CERTIFICAT DU POSTE DE CONDUITE RÉVOQUÉ PAR L'AUTORITÉ CENTRALE/ Marquer les Clés de Mise à Jour comme Non Valides
CONTROLLING STATION'S CERTIFICATE EXPIRED/ No Operation	CERTIFICAT DU POSTE DE CONDUITE EXPIRÉ/ Pas d'Opération
CONTROLLING STATION IS SOLICITED TO PERFORM THE STATION ASSOCIATION - CONTROLLING STATION CERTIFICATE IS NOT VALID OR NOT AVAILABLE/ No Operation	IL EST DEMANDÉ AU POSTE DE CONDUITE DE RÉALISER L'ASSOCIATION DE POSTE – LE CERTIFICAT DU POSTE DE CONDUITE N'EST PAS VALIDE OU NON DISPONIBLE/ Pas d'Opération
KEY MANAGEMENT IDLE	ÉTAT INACTIF DE GESTION DE CLÉS
This state is shared with the Session Key Change state machine	Cet état est partagé avec le diagramme d'état Modification de Clé de Session
CONTROLLED STATION'S CERTIFICATE EXPIRED/ No Operation	CERTIFICAT DU POSTE TÉLÉCONDUIT EXPIRÉ/ Pas d'Opération
CONTROLLED STATION'S CERTIFICATE REVOKED BY THE CENTRAL AUTHORITY/ Mark Update Keys Not Valid	CERTIFICAT DU POSTE TÉLÉCONDUIT RÉVOQUÉ PAR L'AUTORITÉ CENTRALE/ Marquer les Clés de Mise à Jour comme Non Valides
CONTROLLING STATION IS SOLICITED TO PERFORM THE STATION ASSOCIATION - CONTROLLING STATION CERTIFICATE IS VALID	IL EST DEMANDÉ AU POSTE DE CONDUITE DE RÉALISER L'ASSOCIATION DE POSTE – LE CERTIFICAT DU POSTE DE CONDUITE EST VALIDE
Tx Association Request/ Start Reply Timer	Requête d'Association Tx/ Enclencher l'Horloge de Réponse
COMMUNICATION FAILURE DETECTED/ No Operation	ÉCHEC DE COMMUNICATION DÉTECTÉ/ Pas d'Opération
WAIT FOR SESSION RESPONSE	ATTENDRE LA RÉPONSE DE SESSION
Session Key Change State Machine	Diagramme d'état Modification de Clé de Session
MAX REPLY TIMEOUT OR COMMUNICATION FAILURE DETECTED	NOMBRE MAXIMAL DE TEMPORISATIONS DE RÉPONSE OU ÉCHEC DE COMMUNICATION DÉTECTÉ
Failure detected	Échec détecté
Stop Reply Timer	Arrêter l'Horloge de Réponse
Reset Max Reply Timeout Threshold	Réinitialiser le seuil du Nombre maximal de temporisations de réponse
Increment Station Association Failures statistic	Incrémenter la statistique d'échecs d'association de poste
RX VALID UPDATE UPDATE KEY CHANGE RESPONSE	Réponse de modification de Clé de Mise à Jour valide Rx RÉPONSE DE MODIFICATION DE CLÉ DE MISE À JOUR VALIDE Rx
Stop Reply Timer	Arrêter l'Horloge de Réponse
Mark Update Keys as Valid	Marquer les Clés de Mise à Jour comme Valides
Reset Max Reply Timeout Threshold	Réinitialiser le seuil du Nombre maximal de temporisations de réponse
Tx Session Request	Requête de Session Tx
Increment Successful Station Associations statistic	Incrémenter la statistique Associations de Poste Réussies

REPLY TIMEOUT	TEMPORISATION DE RÉPONSE
Increment Reply Timeout Statistic	Incrémenter la statistique Temporisations de Réponse
WAIT FOR ASSOCIATION RESPONSE	ATTENDRE LA RÉPONSE D'ASSOCIATION
RX INVALID ASSOCIATION RESPONSE	RÉPONSE D'ASSOCIATION NON VALIDE Rx
Discard the message	Ignorer le message
RX VALID ASSOCIATION RESPONSE	RÉPONSE D'ASSOCIATION VALIDE Rx
Generate New Update Keys	Générer de nouvelles Clés de Mise à Jour
Tx Update Key Change Request	Requête de Modification de Clé de Mise à Jour Tx
WAIT FOR UPDATE KEY CHANGE RESPONSE	ATTENDRE LA RÉPONSE DE MODIFICATION DE CLÉS DE MISE À JOUR
RX INVALID UPDATE KEY CHANGE RESPONSE	RÉPONSE DE MODIFICATION DE CLÉS DE MISE À JOUR NON VALIDE RX

Figure 4 – Association de Poste – Diagramme d'état du poste de conduite

Tableau 15 – Diagramme d'état du poste de conduite: Association de Poste

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Modification de Clé de Session)		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Il est demandé au poste de conduite de réaliser l'Association de Poste	L'Autorité Centrale ou l'Application a demandé de réaliser la procédure d'Association de Poste.	SI le certificat du poste téléconduit est Valide: – Transmettre le message de Requête de Session. – Enclencher l'Horloge de réponse	Attendre la Réponse d'Association	Ignorer l'événement. (Le poste de conduite exécute déjà la procédure dans cet état)	Attendre la Réponse d'Association	Ignorer l'événement. (Le poste de conduite exécute déjà la procédure dans cet état)	Attendre la Réponse de Modification de Clé de Mise à Jour	1
		SI le certificat du poste téléconduit n'est Pas Valide ou n'est Pas Disponible: – Pas d'Opération	État Inactif de Gestion de Clés					
Réponse d'Association Valide Rx	Le poste de conduite a reçu un message de Réponse d'Association avec des paramètres valides et un certificat de poste téléconduit valide.	Incrémenter la statistique *Messages inattendus*. Ignorer le message. Incrémenter la statistique *Messages ignorés*.	État Inactif de Gestion de Clés	Arrêter l'Horloge de réponse Générer la nouvelle Clé de Mise à Jour Transmettre le message de Requête de Modification de Clé de Mise à Jour. Enclencher l'Horloge de réponse.	Attendre la Réponse de Modification de Clé de Mise à Jour	Incrémenter la statistique *Messages inattendus*. Ignorer le message. Incrémenter la statistique *Messages ignorés*.	Attendre la Réponse de Modification de Clé de Mise à Jour	2

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Modification de Clé de Session)**		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse d'Association Non Valide Rx: le message contient une ou plusieurs erreurs de paramètres.	Le poste de conduite a reçu une Réponse d'Association avec l'une des conditions d'erreur suivantes: a) L'ID d'Association du poste de conduite ne correspond pas à celle de la Requête d'Association b) La Longueur des Données Aléatoires est inférieure à la longueur minimale exigée c) La Longueur des Données Aléatoires est supérieure à la longueur maximale admise.	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages ignorés.*	État Inactif de Gestion de Clés	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages ignorés.*	Attendre la Réponse d'Association	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages ignorés.*	Attendre la Réponse de Modification de Clé de Mise à Jour	3

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Modification de Clé de Session)		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse d'Association Non Valide Rx: le certificat du poste téléconduit n'est PAS valide.	Le poste de conduite a reçu une Réponse d'Association avec l'une des conditions d'erreur suivantes: a) Le certificat du poste téléconduit a expiré. b) Le certificat du poste téléconduit est révoqué par l'Autorité Centrale. c) La signature du certificat du poste téléconduit n'est pas valide. d) La longueur de la clé publique est inférieure à la longueur minimale exigée. e) La Courbe EC spécifiée n'est pas admise ou n'est pas prise en charge, ou ne correspondant pas à la courbe EC spécifiée dans ce certificat du poste de conduite.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Incrémenter la statistique *Échecs de vérification de Validité du Certificat du Poste Distant*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse d'Association	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Mise à Jour	4

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Modification de Clé de Session)		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse d'Association Non Valide Rx: le poste téléconduit n'est pas autorisé à communiquer.	Le poste de conduite a reçu une Réponse d'Association avec l'une des conditions d'erreur suivantes: a) Le certificat du poste téléconduit est signé par la CA et le certificat CA correspondant n'est pas fourni à ce poste de conduite. b) Le certificat du poste téléconduit est autosigné et la clé publique correspondante n'est pas fournie à ce poste de conduite. c) Le certificat du poste téléconduit est signé par la CA et aucune chaîne AoR du certificat du poste téléconduit ne correspond aux chaînes AoR assignées à ce poste de conduite. d) Le certificat du poste téléconduit identifie un poste non autorisé à communiquer avec ce poste de conduite par configuration.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Incrémenter la statistique *Échecs d'Autorisation du Poste Distant*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse d'Association	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Mise à Jour	5

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Modification de Clé de Session)**		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse de Modification de Clé de Mise à Jour Valide Rx	Le poste de conduite a reçu une Réponse de Modification de Clé de Mise à Jour correctement authentifiée avec des paramètres valides.	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages Ignorés.*	État Inactif de Gestion de Clés	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages Ignorés.*	Attendre la Réponse d'Association	Arrêter l'Horloge de réponse Marquer la Clé de Mise à Jour comme Valide. Incrémenter la statistique *Association de Poste Réussie.* Réinitialiser le seuil du Nombre Maximal de Temporisations de Réponses Transmettre le message de Requête de Session. Enclencher l'Horloge de réponse	Attendre la Réponse de Session (Procédure de Modification de Clé de Session)	**6**
Réponse de Modification de Clé de Mise à Jour Non Valide Rx: le message n'est pas authentique.	Le poste de conduite a reçu un message de Réponse de Modification de Clé de Mise à Jour avec une information d'authentification non valide.	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages Ignorés.*	État Inactif de Gestion de Clés	Incrémenter la statistique *Messages Inattendus.* Ignorer le message. Incrémenter la statistique *Messages Ignorés.*	Attendre la Réponse d'Association	Incrémenter la statistique *Erreurs d'Authentification des Clés.* Ignorer le message. Incrémenter la statistique *Messages Ignorés.*	Attendre la Réponse de Modification de Clé de Mise à Jour	**7**

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Modification de Clé de Session)**		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse de Modification de Clé de Mise à Jour Non Valide Rx: le message contient une ou plusieurs erreurs de paramètres	Le poste de conduite a reçu une Réponse de Modification de Clé de Mise à Jour correctement authentifiée avec l'une des conditions d'erreur suivantes: a) L'ID d'Association du poste de conduite est incorrecte. b) L'ID d'Association du poste téléconduit est incorrecte.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse d'Association	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Mise à Jour	**8**
Temporisation de réponse	L'Horloge de réponse a expiré alors que le poste de conduite attendait une réponse du poste téléconduit, et la statistique Reply Timeouts n'a pas atteint le seuil Max Reply Timeouts.	Ignorer l'événement. (Cet événement ne peut se produire que lorsque l'état du diagramme d'état est "*Attendre la Réponse d'Association*" ou "*Attendre la Réponse de Modification de Clé de Mise à Jour*)	État Inactif de Gestion de Clés	Incrémenter la statistique *Temporisations de Réponse*. Transmettre le message de Requête d'Association Enclencher l'Horloge de réponse.	Attendre la Réponse d'Association	Incrémenter la statistique *Temporisations de Réponse*. Transmettre à nouveau le dernier message de Requête de Modification de Clé de Mise à Jour. Enclencher l'Horloge de réponse.	Attendre la Réponse de Modification de Clé de Mise à Jour	**9**

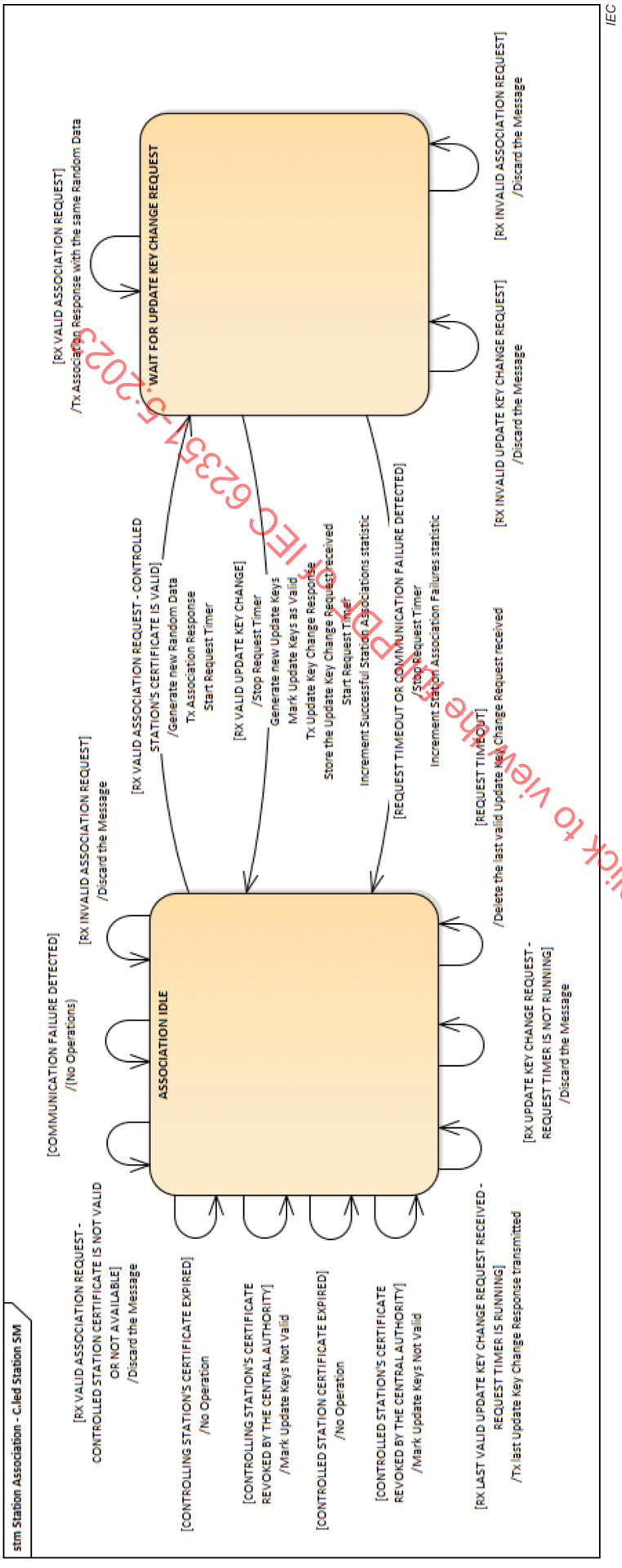
Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Modification de Clé de Session)**		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Nombre Maximal de Temporisations de Réponses	La procédure actuelle d'association d'estacion a échoué parce que la statistique Temporisation de Réponse a atteint le seuil du nombre Maximal de Temporisations de Réponses alors que le poste de conduite attendait une réponse du poste téléconduit.	Ignorer l'événement. (Cet événement ne peut se produire que lorsque l'état du diagramme d'état est "*Attendre la Réponse de Session*" ou "*Attendre la Réponse de Modification de Clé de Session*)	État Inactif de Gestion de Clés	Incrémenter la statistique *Nombre Maximal de Temporisations de Réponses*. Réinitialiser le seuil du Nombre Maximal de Temporisations de Réponses. Incrémenter la statistique *Échecs d'Association de Poste*	État Inactif de Gestion de Clés	Incrémenter la statistique *Nombre Maximal de Temporisations de Réponses*. Réinitialiser le seuil du Nombre Maximal de Temporisations de Réponses. Incrémenter la statistique *Échecs d'Association de Poste*	État Inactif de Gestion de Clés	**10**
Échec de communication détecté Note: cet événement doit être pris en compte si des défaillances de communication peuvent être détectées dans la liaison de communication.	Le poste a détecté un échec de communication.	Pas d'Opération.	État Inactif de Gestion de Clés	Arrêter l'Horloge de réponse. Réinitialiser le seuil du Nombre Maximal de Temporisations de Réponses Incrémenter la statistique *Échecs d'Association de Poste*.	État Inactif de Gestion de Clés	Arrêter l'Horloge de réponse. Réinitialiser le seuil du Nombre Maximal de Temporisations de Réponses Incrémenter la statistique *Échecs d'Association de Poste*.	État Inactif de Gestion de Clés	**11**

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Modification de Clé de Session)**		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Le certificat du poste de conduite a été révoqué.	Le certificat du poste de conduite a été révoqué par l'Autorité Centrale à l'établissement de l'Association de Poste.	Marquer les Clés de Mise à Jour comme Non Valides Incrémenter la statistique *Révocations du Certificat du Poste Local*. Incrémenter la statistique *Invalidations des Clés Cryptographiques dues à la Révocation du Certificat du Poste Local*.	État Inactif de Gestion de Clés	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse de Modification de Clé de Mise à Jour	**12**
Le certificat du poste de conduite a expiré.	La validité du certificat du poste de conduite a expiré à l'établissement de l'Association de Poste.	Aucune autre opération n'est exigée si ce n'est l'opération Incrémenter la statistique Expirations du Certificat du Poste Local.	État Inactif de Gestion de Clés	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse de Modification de Clé de Mise à Jour	**13**

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Modification de Clé de Session)		**Attendre la Réponse d'Association**		**Attendre la Réponse de Modification de Clé de Mise à Jour**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête d'Association		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Mise à Jour.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Le certificat du poste téléconduit a été révoqué.	Le certificat du poste téléconduit a été révoqué par l'Autorité Centrale à l'établissement de l'Association de Poste.	Marquer les Clés de Mise à Jour comme Non Valides Incrémenter la statistique *Révocations du Certificat du Poste Distant*. Incrémenter la statistique *Invalidations des Clés Cryptographiques dues à la Révocation du Certificat du Poste Distant*.	État Inactif de Gestion de Clés	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse de Modification de Clé de Mise à Jour	**14**
Le certificat du poste téléconduit a expiré.	La validité du certificat du poste téléconduit a expiré à l'établissement de l'Association de Poste.	Aucune autre opération n'est exigée si ce n'est l'opération Incrémenter la statistique Expirations du Certificat du Poste Distant.	État Inactif de Gestion de Clés	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Réponse de Modification de Clé de Mise à Jour	**15**

8.3.7 Diagramme d'état du poste téléconduit

Sur le poste téléconduit, les messages de la procédure d'Association de Poste décrits en 8.3.5 doivent être gérés par le diagramme d'état décrit en 8.3.7. La Figure 5 représente les transactions de l'Association de Poste sur le poste téléconduit. Le poste téléconduit doit exécuter le diagramme d'état Association de Poste décrit dans le Tableau 16.



Anglais	Français
COMMUNICATION FAILURE DETECTED/ No Operations	ÉCHEC DE COMMUNICATION DÉTECTÉ/ Pas d'Opération
RX VALID ASSOCIATION REQUEST – CONTROLLED STATION CERTIFICATE IS NOT VALID OR NOT AVAILABLE/ Discard the Message	REQUÊTE D'ASSOCIATION VALIDE Rx - LE CERTIFICAT DU POSTE TÉLÉCONDUIT N'EST PAS VALIDE OU PAS DISPONIBLE/ Ignorer le Message
RX INVALID ASSOCIATION REQUEST/ Discard the Message	REQUÊTE D'ASSOCIATION NON VALIDE Rx/ Ignorer le Message
Tx Association Response with the same Random Data	Réponse d'Association Tx avec les mêmes Données Aléatoires
CONTROLLING STATION'S CERTIFICATE EXPIRED/ No Operation	LE CERTIFICAT DU POSTE DE CONDUITE A EXPIRÉ/ Pas d'Opération
ASSOCIATION IDLE	ÉTAT INACTIF D'ASSOCIATION
CONTROLLED STATION'S CERTIFCATE IS VALID	LE CERTIFICAT DU POSTE TÉLÉCONDUIT EST VALIDE
Generate new Random Data/ Tx Association Response/ Start Request Timer	Générer de nouvelles Données Aléatoires/ Réponse d'Association Tx/ Enclencher l'Horloge de Requête
WAIT FOR UPDATE KEY CHANGE REQUEST	ATTENDRE LA REQUÊTE DE MODIFICATION DE CLÉ DE MISE À JOUR
CONTROLLING STATION'S CERTIFICATE REVOKED BY THE CENTRAL AUTHORITY/ Mark Update Keys Not Valid	CERTIFICAT DU POSTE DE CONDUITE RÉVOQUÉ PAR L'AUTORITÉ CENTRALE/ Marquer les Clés de Mise à Jour comme Non Valides
Rx VALID UPDATE KEY CHANGE/ Stop Request Timer/ Generate new Update Keys/ Mark Update Keys as Valid/ Tx Update Key Change Response/ Store the Update Key Change Request received/ Increment Successful Station Associations statistic	MODIFICATION DE CLÉS DE MISE À JOUR VALIDE RX/ Arrêter l'Horloge de Requête/ Générer de nouvelles Clés de Mise à Jour/ Marquer les Clés de Mise à Jour comme Valides/ Réponse de Modification de Clés de Mise à Jour Tx/ Archiver la Requête de Modification de Clés de Mise à Jour reçue/ Incrémenter la statistique Associations de Postes Réussies
CONTROLLED STATION CERTIFICATE EXPIRED	CERTIFICAT DU POSTE TÉLÉCONDUIT EXPIRÉ
CONTROLLED STATION'S CERTIFICATE REVOKED BY THE CENTRAL AUTHORITY	CERTIFICAT DU POSTE TÉLÉCONDUIT RÉVOQUÉ PAR L'AUTORITÉ CENTRALE
REQUEST TIMEOUT OR COMMUNICATION FAILURE DETECTED/ Increment Station Associations Failures statistic	TEMPORISATION DE REQUÊTE OU ÉCHEC DE COMMUNICATION DÉTECTÉ/ Incrémenter la statistique Échecs d'Associations de Postes
RX LAST VALID UPDATE KEY CHANGE REQUEST RECEIVED – REQUEST TIMER IS RUNNING/ Tx last Update Key Change Response transmitted	DERNIÈRE REQUÊTE DE MODIFICATION DE CLÉS DE MISE À JOUR VALIDE RX REÇUE – L'HORLOGE DE REQUÊTE FONCTIONNE/ Dernière Réponse de Modification de Clés de Mise à Jour Tx transmise
RX UPDATE KEY CHANGE REQUEST – REQUEST TIMER IS NOT RUNNING	REQUÊTE DE MODIFICATION DE CLÉ DE MISE À JOUR RX - L'HORLOGE DE REQUÊTE NE FONCTIONNE PAS
REQUEST TIMEOUT/ Delete the last valid Update Key Change Request received	TEMPORISATION DE REQUÊTE/ Supprimer la dernière Requête de Modification de Clés de Mise à Jour reçue
RX INVALID UPDATE KEY CHANGE REQUEST	REQUÊTE DE MODIFICATION DE CLÉS DE MISE À JOUR NON VALIDE RX

Figure 5 – Association de Poste – Diagramme d'état du poste téléconduit

Tableau 16 – Diagramme d'état du poste téléconduit: Association de Poste

Événement	Description de l'événement	État				
		État inactif d'Association		**Attendre la Requête de Modification de Clé de Mise à Jour**		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	
Requête d'Association Valide Rx	Le poste téléconduit a reçu une Requête d'Association valide.	SI le certificat du poste téléconduit est Valide: – Générer les nouvelles données aléatoires à transmettre. – Transmettre la Réponse d'Association avec les nouvelles données aléatoires générées. – Enclencher l'Horloge de Requête	Attendre la Requête de Modification de Clé de Mise à Jour	Transmettre la Réponse d'Association avec les mêmes données aléatoires fournies dans la dernière Réponse d'Association transmise.	Attendre la Requête de Modification de Clé de Mise à Jour	**1**
		SI le certificat du poste téléconduit n'est Pas Valide ou n'est Pas Disponible: – Ignorer le message – Incrémenter la statistique *Messages ignorés*	État inactif d'Association			**2**
Requête d'Association Non Valide Rx: Erreur d'Information de Protocole.	Le poste téléconduit reçoit une Requête d'Association qui spécifie une valeur d'Information de Protocole qui n'est pas admise ou n'est pas prise en charge	Incrémenter la statistique *Erreurs d'Information de Protocole* Ignorer le message Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Erreurs d'Information de Protocole* Ignorer le message Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	**3**

Événement	Description de l'événement	État				
		État inactif d'Association		Attendre la Requête de Modification de Clé de Mise à Jour		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	État Suivant	Action	État Suivant	
A	B	C	D	E	F	
Requête d'Association Non Valide Rx: le certificat du poste de conduite n'est PAS valide.	Le poste téléconduit a reçu une Requête d'Association avec l'une des conditions d'erreur suivantes: a) Le certificat du poste de conduite a expiré. b) Le certificat du poste de conduite est révoqué par l'Autorité Centrale. c) La signature du certificat du poste de conduite n'est pas valide. d) La longueur de la clé publique est inférieure à la longueur minimale exigée. e) La Courbe EC spécifiée n'est pas admise ou n'est pas prise en charge, ou ne correspondant pas à la courbe EC spécifiée dans ce certificat du poste de conduite.	Incrémenter la statistique *Échecs de vérification de Validité du Certificat du Poste Distant*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Échecs de vérification de Validité du Certificat du Poste Distant*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	4

Requête d'Association Non Valide Rx: le poste de conduite n'est pas autorisé à communiquer.	Le poste téléconduit a reçu une Requête d'Association avec l'une des conditions d'erreur suivantes: a) Le certificat du poste de conduite est signé par la CA et le certificat CA correspondant n'est pas fourni à ce poste téléconduit. b) Le certificat du poste de conduite est autosigné et la clé publique correspondante n'est pas fournie à ce poste téléconduit. c) Le certificat du poste téléconduit est signé par la CA et aucune chaîne AoR du certificat du poste de conduite ne correspond aux chaînes AoR assignées à ce poste téléconduit d) Le certificat du poste de conduite identifie un poste non autorisé à communiquer avec ce poste de conduite par configuration	*Incrémenter la statistique Échecs d'Autorisation du Poste Distant* Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	*Incrémenter la statistique Échecs d'Autorisation du Poste Distant* Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	**5**
Requête de Modification de Clé de Mise à Jour Valide Rx	Le poste téléconduit a reçu une Requête de Modification de Clé de Mise à Jour correctement authentifiée avec des paramètres valides.	SI l'Horloge de Requête fonctionne ET la Requête de Modification de Clé de Mise à Jour est identique à la dernière Requête de Modification de Clé de Mise à Jour valide reçue: – Retransmettre la Réponse de Modification de Clé de Mise à Jour transmise le plus récemment SINON:	État inactif d'Association	Arrêter l'Horloge de Requête. Générer les nouvelles Clés de Mise à Jour Marquer les Clés de Mise à Jour comme Valides Transmettre la Réponse de Modification de Clé de Mise à Jour. Archiver la Requête de Modification de Clé de Mise à Jour reçue	État inactif d'Association	**6**

Événement	Description de l'événement	État				
		État inactif d'Association		Attendre la Requête de Modification de Clé de Mise à Jour		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	État Suivant	Action	État Suivant	
A	B	C	D	E	F	
		– Incrémenter la statistique *Messages Inattendus*. – Ignorer le message. – Incrémenter la statistique *Messages ignorés*		Enclencher l'Horloge de Requête Incrémenter la statistique *Associations de Poste Réussies*.		
Requête de Modification de Clé de Mise à Jour Non Valide Rx: le message n'est PAS authentique.	Le poste téléconduit a reçu un message de Requête de Modification de Clé de Mise à Jour avec une information d'authentification non valide.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Erreurs d'Authentification des Clés*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	7

Événement	Description de l'événement	État				
		État inactif d'Association		Attendre la Requête de Modification de Clé de Mise à Jour		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	État Suivant	Action	État Suivant	
A	B	C	D	E	F	
Requête de Modification de Clé de Mise à Jour Non Valide Rx: le message contient une ou plusieurs erreurs de paramètres.	Le poste téléconduit reçoit une Requête de Modification de Clé de Mise à Jour correctement authentifiée avec l'une des conditions d'erreur suivantes: a) L'ID d'Association du poste téléconduit ne correspond pas à celle de la dernière Réponse d'Association transmise b) La Longueur des Données Aléatoires est inférieure à la longueur minimale exigée c) La Longueur des Données Aléatoires est supérieure à la longueur maximale admise.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	8
Requête de Modification de Clé de Mise à Jour Non Valide Rx: Algorithme d'authentification de clés non admis.	Le poste téléconduit reçoit une Requête de Modification de Clé de Mise à Jour correctement authentifiée qui définit un algorithme d'authentification de clés (MAL) non admis ou non pris en charge.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Erreurs de Prise en charge de l'Algorithme d'Authentification de Clés*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	9

Événement	Description de l'événement	État				
		État inactif d'Association		**Attendre la Requête de Modification de Clé de Mise à Jour**		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	
Requête de Modification de Clé de Mise à Jour Non Valide Rx: Algorithme d'enveloppement de clés non admis.	Le poste téléconduit reçoit une Requête de Modification de Clé de Mise à Jour correctement authentifiée qui définit un algorithme d'enveloppement de clés (KWA - *Key Wrap Algorithm*) non admis ou non pris en charge.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État inactif d'Association	Incrémenter la statistique *Erreurs de Prise en charge de l'Algorithme d'Enveloppement de Clés*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Requête de Modification de Clé de Mise à Jour	**10**
Temporisation de requête	L'Horloge de Requête a expiré alors que le poste téléconduit attendait une Requête de Modification de Clé de Mise à Jour valide du poste de conduite.	Supprimer la dernière Requête de Modification de Clé de Mise à Jour valide reçue.	État inactif d'Association	Incrémenter la statistique *Temporisations de Requête*. Incrémenter la statistique *Échecs d'Association de Poste*.	État inactif d'Association	**11**
Échec de communication détecté Note: cet événement doit être pris en compte si des défaillances de communication peuvent être détectées dans la liaison de communication	Le poste téléconduit a détecté un échec de communication	Pas d'Opérations.	État inactif d'Association	Arrêter l'Horloge de Requête. Incrémenter la statistique *Échecs d'Association de Poste*.	Pas d'Association	**12**

Événement	Description de l'événement	État				
		État inactif d'Association		Attendre la Requête de Modification de Clé de Mise à Jour		
		État stable pour la gestion de l'Association de Poste et des Clés de Mise à Jour Le poste téléconduit n'a pas reçu de Requête d'Association valide de la part du poste de conduite		Le poste téléconduit attend une Requête de Modification de Clé de Mise à Jour de la part du poste de conduite		
		Action	État Suivant	Action	État Suivant	
A	B	C	D	E	F	
Le certificat du poste de conduite a été révoqué.	Le certificat du poste de conduite a été révoqué par l'Autorité Centrale.	Marquer les Clés de Mise à Jour comme Non Valides Incrémenter la statistique *Révocations du Certificat du Poste Distant*. Incrémenter la statistique *Invalidations des Clés Cryptographiques dues à la Révocation du Certificat du Poste Distant*	État inactif d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Requête de Modification de Clé de Mise à Jour	**13**
Le certificat du poste de conduite a expiré.	La validité du certificat du poste de conduite a expiré.	Aucune autre opération n'est exigée si ce n'est l'opération Incrémenter la statistique *Expirations du Certificat du Poste Distant*.	État inactif d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Requête de Modification de Clé de Mise à Jour	**14**
Le certificat du poste téléconduit a été révoqué.	Le certificat du poste de conduite a été révoqué par l'Autorité Centrale.	Marquer les Clés de Mise à Jour comme Non Valides Incrémenter la statistique *Révocations du Certificat du Poste Local* Incrémenter la statistique *Invalidations des Clés Cryptographiques dues à la Révocation du Certificat du Poste Local*	État inactif d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Requête de Modification de Clé de Mise à Jour	**15**
Le certificat du poste téléconduit a expiré.	La validité du certificat du poste de conduite a expiré.	Aucune autre opération n'est exigée si ce n'est l'opération Incrémenter la statistique Expirations du Certificat du Poste Local.	État inactif d'Association	Cette condition ne doit pas être vérifiée dans cet état puisque la nouvelle Association de Poste n'est pas encore établie.	Attendre la Requête de Modification de Clé de Mise à Jour	**16**

8.3.8 Vérification du certificat du poste distant

8.3.8.1 Généralités

Pendant la procédure d'Association de Poste, le poste de conduite et le poste téléconduit doivent vérifier la validité du certificat fourni par le poste distant en réalisant l'opération décrite ci-dessous. Des vérifications supplémentaires peuvent être exigées par les normes de référence du protocole concerné (se reporter également à l'IEC 62351-9 Éd. 2 pour la vérification des certificats fournis par la CA).

Si l'une des vérifications de certificats échoue, le poste local doit considérer le certificat du poste distant comme non valide et doit interrompre la Procédure d'Association de Poste (le poste de conduite ne doit pas envoyer le message de Requête de Modification de Clé de Mise à Jour qui suit, le poste téléconduit ne doit pas répondre avec le message de Réponse d'Association).

Si les Clés de Mise à Jour en cours sont valides, le poste local ne doit pas invalider les Clés de Mise à Jour si les vérifications du certificat du poste distant échouent.

Si l'association de station est effectuée avec succès, les données de certificat reçues de la station distante doivent être stockées en permanence sur la station locale, de sorte que cette procédure ne soit pas exécutée après une initialisation de la station ou après une panne de communication.

8.3.8.2 Vérification du certificat autosigné

Si le certificat est autosigné par le dispositif, des opérations supplémentaires doivent être réalisées sur le certificat du poste distant, comme cela est énuméré ci-dessous:

– vérifier la signature numérique du certificat;
– vérifier que la date de début de la validité permet l'utilisation du certificat;
– vérifier que le certificat n'a pas expiré;
– vérifier que la clé publique contenue dans le certificat reçu est fournie au poste local comme cela est décrit en 8.3.4.

8.3.8.3 Vérification du certificat signé par l'autorité centrale

Si l'Autorité Centrale est prise en charge et que le certificat est signé par cette dernière, les opérations suivantes doivent être réalisées sur le certificat du poste distant, comme cela est énuméré ci-dessous (se reporter à l'ISO 62531-9 pour la vérification du certificat):

– vérifier que le certificat a été émis par une Autorité Centrale reconnue. Les Certificats de l'Autorité Centrale doivent être fournis aux postes comme cela est décrit en 8.3.4;
– en cas de réception d'un certificat d'attribut, vérifier que le certificat ID correspondant est fourni au poste local;
– vérifier la signature numérique du certificat;
– vérifier que la date de début de la validité permet l'utilisation du certificat;
– vérifier que le certificat n'a pas expiré;
– vérifier que le certificat n'est pas révoqué par l'Autorité Centrale;
– si le RBAC et la zone de responsabilité (AoR - *Area of Responsibility*) sont pris en charge, vérifier que les chaînes de texte de l'AoR dans le certificat du poste distant correspondent à une chaîne de ce type au moins dans le certificat du poste local;
– de manière facultative, si la liste des postes distants autorisés est configurée, vérifier le Nom Identifié des certificats.

8.3.9 Vérification des certificats pendant les opérations normales

Le poste de conduite et le poste téléconduit doivent être capables de vérifier l'état de leur propre certificat, ainsi que du certificat du poste distant de manière régulière pendant les opérations normales.

Il convient que le poste local vérifie l'expiration de son propre certificat et du certificat du poste distant au moins toutes les 24 h.

De plus, si l'Autorité Centrale est prise en charge et que les certificats signés par cette dernière sont utilisés dans la procédure d'Association de Poste, il convient que le poste local vérifie l'état de révocation de son propre certificat, ainsi que du certificat du poste distant au moins toutes les 24 h. La méthode utilisée pour vérifier la révocation du certificat ne relève pas du domaine d'application du présent document. Il convient qu'elle suive les directives définies dans l'IEC 62351-9. D'autres méthodes de vérification de l'état de révocation des certificats peuvent être définies dans les normes de référence du protocole concerné.

Si le certificat du poste local ou le certificat du poste distant expire pendant que les Clés de Mise à Jour sont valides, le poste local ne doit pas invalider les Clés de Mise à Jour.

Si le certificat du poste local ou le certificat du poste distant est révoqué par l'Autorité Centrale pendant que les Clés de Mise à Jour sont valides, le poste local doit invalider les Clés de Mise à Jour et les Clés de Session des associations établies avec ce certificat.

L'Autorité Centrale doit fournir un nouveau certificat à chaque poste avant que son certificat n'expire ou ne soit révoqué. Lorsqu'un nouveau certificat est fourni soit au poste de conduite soit au poste téléconduit, il doit être demandé au poste de conduite de déclencher la procédure d'Association de Poste dès que possible.

8.3.10 Dérivation des Clés de Mise à Jour

Le poste de conduite et le poste téléconduit doivent générer les Clés de Mise à Jour comme cela est décrit en 8.3.10.

Le poste de conduite dérive les Clés de Mise à Jour après avoir reçu le message de Réponse d'Association du poste téléconduit et avoir généré les données aléatoires pour le prochain message de Requête de Modification de Clé de Mise à Jour à envoyer. Le poste téléconduit dérive les Clés de Mise à Jour lorsqu'il reçoit un message de Requête de Modification de Clé de Mise à Jour.

La taille des clés de mise à jour est de 256 bits (32 octets) car les algorithmes sélectionnés dans les champs KWA et MAL du message de demande de changement de clé de mise à jour, décrit au 8.3.5.4, nécessitent des clés de 256 bits. Les dispositifs doivent dériver les Clés de Mise à Jour conformément au document RFC 5869:

1) les dispositifs échangent leur certificat X.509 et leurs données aléatoires récemment générées pendant la procédure d'Association de Poste comme cela est décrit en 8.3.5;
2) chaque dispositif réalise la même fonction de multiplication scalaire sur sa propre clé privée et sur la clé publique de l'autre dispositif afin de produire le matériau de modulation intermédiaire IKM (K dans le document RFC 7748);

   NOTE Pour chaque connexion poste de conduite/poste téléconduit, la valeur de IKM ne varie pas, sauf si l'un des deux côtés modifie ses données de certificat/clé privée.

3) chaque dispositif doit concaténer les Données Aléatoires échangées, ainsi que les données aléatoires du poste de conduite et du poste téléconduit dans cet ordre, afin de produire la valeur Salt;

4) chaque dispositif doit réaliser la fonction HKDF Extraire (Salt, IKM) afin de produire la Clé Pseudoaléatoire (PRK);
5) chaque dispositif doit réaliser la fonction HKDF Étendre (PRK, Info, L) afin de produire une valeur T longue de L octets. La valeur du paramètre L doit être 64 de telle manière que 64 octets soient générés comme sortie par cette fonction. Le paramètre Info doit être une chaîne de longueur zéro;
6) les 32 premiers octets de T, T[1], doivent être la Clé de Mise à Jour de Chiffrement utilisée pour chiffrer les Clés de Session dans la procédure de Modification de Clé de Session décrite en 8.4;
7) les 32 derniers octets de T, T[2], doivent être la Clé de Mise à Jour d'Authentification utilisée pour calculer le MAC afin d'authentifier les messages échangés dans la procédure d'Association de Poste en cours de réalisation, décrite en 8.3, ainsi que dans les procédures de Modification de Clé de Session réalisées par la suite, décrites en 8.4.

Les Clés de Mise à Jour dérivées et l'ID d'Association correspondante qui a fait l'objet d'un accord pendant la procédure d'Association de Poste doivent être stockées de manière permanente sur chaque poste, de telle manière que cette procédure ne doit pas être exécutée après l'initialisation d'un poste ou après un échec de communication.

8.3.11 Directives du poste de conduite pour la gestion de l'Association de Poste et des Clés de Mise à Jour

Le poste de conduite doit initier la procédure d'Association de Poste dès que possible lorsque la communication avec le poste téléconduit est établie si les Clés de Mise à Jour ne sont pas initialisées ou sont non valides, ou lorsque cela est demandé par l'Autorité Centrale, ou par l'application.

Si la procédure d'Association de Poste échoue, le poste de conduite ne doit pas tenter la procédure de nouveau de manière automatique: le poste de conduite doit avertir l'organisation de l'échec pour que le personnel autorisé puisse prendre les mesures nécessaires. Les méthodes possibles pour signaler l'échec d'une Association de Poste sont décrites en 7.5.

Si les Clés de Mise à Jour en cours sont valides, le poste de conduite ne doit pas les invalider lorsqu'il initie une nouvelle procédure d'Association de Poste ou lorsque cette procédure échoue. Le poste de conduite doit plutôt examiner les Clés de Mise à Jour toujours valides en cours jusqu'à ce que la procédure d'Association de Poste suivante ait été réalisée avec succès (c'est-à-dire que le poste de conduite reçoit un message de Réponse de Modification de Clé de Mise à Jour valide). Chaque fois qu'une procédure d'Association de Poste a été réalisée avec succès, le poste de conduite doit utiliser les nouvelles Clés de Mise à Jour générées pour modifier les Clés de Session dans toutes les procédures suivantes de Modification de Clé de Session, comme cela est décrit en 8.4.

8.3.12 Directives du poste téléconduit pour la gestion de l'Association de Poste et des Clés de Mise à Jour

8.3.12.1 Généralités

Le poste téléconduit doit attendre le poste de conduite pour initier la procédure d'Association de Poste si les Clés de Mise à Jour ne sont pas initialisées ou sont non valides.

De manière facultative, le poste téléconduit peut demander au poste de conduite d'initier une procédure d'Association de Poste par l'envoi d'un message de Requête d'Initiation d'Association au poste de conduite comme cela est décrit en 8.3.5.6.

Si les Clés de Mise à Jour en cours sont valides, le poste téléconduit ne doit pas les invalider lorsqu'il reçoit un message de Requête d'Association du poste de conduite ou lorsque la procédure d'Association de Poste échoue. Le poste téléconduit doit plutôt prendre en considération les Clés de Mise à Jour toujours valides en cours jusqu'à ce qu'il reçoive du poste de conduite un message de Requête de Modification de Clé de Mise à Jour valide. Il doit alors générer et utiliser les nouvelles Clés de Mise à Jour pour modifier les Clés de Session dans toutes les procédures suivantes de Modification de Clé de Session, comme cela est décrit en 8.4.

Il est fortement recommandé que le poste téléconduit limite le nombre d'associations prises en charge simultanément. Le poste satellite est autorisé à ne pas répondre à une Requête d'Association quelconque si cette limite est dépassée.

8.3.12.2 Gestion du Contrôle d'Accès Basé sur les Rôles (RBAC) sur le poste téléconduit

8.3.12.2.1 Généralités

Le support du mécanisme RBAC est optionnel. Si le poste téléconduit prend en charge le mécanisme RBAC, celui-ci doit être mis en œuvre comme cela est décrit en 8.3.12.2.

Sur le poste téléconduit, chaque poste de conduite autorisé à communiquer a des rôles et des permissions associés. Le Rôle du poste de conduite doit déterminer quelles actions il est autorisé à réaliser sur le poste téléconduit. Le Tableau 17 décrit l'ensemble minimal de rôles types et les permissions correspondantes à prendre en charge. Ces rôles sont alignés sur ceux définis dans l'IEC 62351-8 et les permissions sont spécifiques à la présente norme. Les mises en œuvre peuvent donner lieu à l'introduction de rôles et de permissions supplémentaires dans la plage privée, comme cela est défini dans l'IEC 62351-8. Le mécanisme qui définit les rôles définis supplémentaires est décrit dans l'IEC 62351-8 *RoleDefinition* est un champ obligatoire et doit être réglé par rapport à l'IEC 62351-5 pour les rôles décrits dans le présent document. *Revision* est également un champ obligatoire et doit être réglé sur 0. Les champs *RoleDefinition* et *Revision* font partie intégrante du jeton d'accès défini dans l'IEC 62351-8.

Tableau 17 – Liste d'affectations rôle-permission prédéfinies

Valeur	Permission / Nom de rôle	MONITOR DATA	OPERATE CONTROLS	FILEREAD	FILEWRITE	FILEMNGT	CONFIG OPERATION PARAMETERS	CONFIG SECURITY PARAMETERS
<0>	VIEWER	X		C_1				
<1>	OPERATOR	X	X	C_1				
<2>	ENGINEER	X		X_1	X_1	X_1	X	
<3>	INSTALLER	X		X_2	X_2		X	
<4>	SECADM			X_4	X_4	X_4		X
<5>	SECAUD			X_3				
<6>	RBACMNT			X_4	X_4	X_4		X
<7…32767>	Réservé	Pour utilisation ultérieure des rôles IEC définis.						
<-32768…-1>	Privé	Défini par accord externe. Interopérabilité non garantie.						

C_1 Accès en lecture conditionnel pour les fichiers de données filetype (peut ne pas avoir accès aux paramètres de sécurité, mais traiter les valeurs)

X_1 Accès aux fichiers de données de type et config

X_2 Accès aux fichiers de configuration de type et microprogramme (mises à jour)

X_3 Accès aux fichiers de journaux d'audit de type

X_4 Accès aux fichiers de sécurité de type (config)

8.3.12.2.2 RBAC utilisant des certificats autosignés

Si des certificats autosignés sont utilisés dans la procédure d'Association de Poste, le poste téléconduit doit permettre que les informations du RBAC soient préconfigurées pour chaque poste de conduite autorisé à communiquer comme cela est décrit en 8.3.2.3. Cette configuration ne doit être permise qu'au personnel autorisé. La méthode de configuration des informations RBAC sur les dispositifs ne relève pas du domaine d'application du présent document.

Si le certificat autosigné contient des informations RBAC, le poste téléconduit doit ignorer ces informations.

8.3.12.2.3 RBAC utilisant un certificat signé par une Autorité Centrale

Si l'Autorité Centrale est prise en charge et si les certificats signés par l'Autorité Centrale sont utilisés dans la procédure d'Association de Poste, le poste téléconduit doit être capable de récupérer et d'archiver les Rôles du poste de conduite auprès de l'extension RBAC dans le certificat du poste de conduite.

À réception du certificat de clé publique du poste de conduite, si le certificat de clé publique ne contient pas d'informations RBAC, le poste téléconduit peut, de manière facultative, aller chercher le certificat d'attribut du poste de conduite qui contient des informations RBAC dans un référentiel externe. La méthode de récupération du certificat d'attribut dans ce type de référentiel (méthode PULL) est décrite dans l'IEC 62351-8.

Pour chaque ID d'Association, l'information RBAC du poste de conduite doit être stockée de manière permanente sur le poste téléconduit chaque fois que la procédure d'Association de Poste a été réalisée avec succès, de telle manière que ces informations soient conservées après une initialisation de poste ou après un échec de communication.

8.3.13 Initialisation et mise à jour d'Associations de Postes et de Clés de Mise à Jour

La Figure 6 représente l'initialisation de l'ID d'Association et des Clés de Mise à Jour correspondantes, suivie par l'initialisation des Clés de Session correspondantes pendant l'enregistrement d'un dispositif ou chaque fois que la procédure d'Association de Poste est exigée.

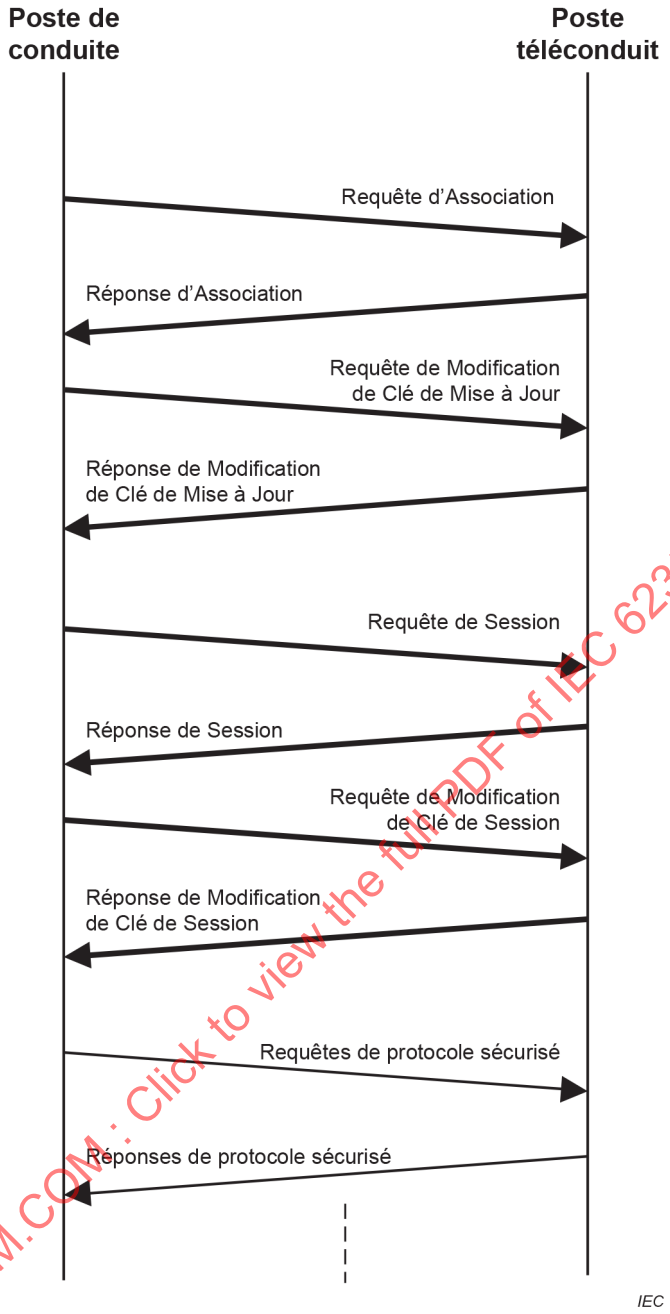


Figure 6 – Exemple d'initialisation d'ID d'Association, de Clés de Mise à Jour et de Clés de Session

8.4 Procédure de Modification de Clé de Session

8.4.1 Généralités

Cette procédure doit être réalisée pour initialiser ou renouveler les clés de Session pour une Association. Chaque dispositif doit maintenir un ensemble unique de Clés de Session pour chaque association poste de conduite/poste téléconduit établie pendant la procédure d'Association de Poste.

Cette procédure ne peut être réalisée que si le poste de conduite et le poste téléconduit comportent les Clés de Mise à Jour qui correspondent à l'ID d'Association.

8.4.2 Définition des messages

8.4.2.1 Généralités

Le paragraphe 8.4.2 décrit les messages de sécurité et les données échangées dans chaque message de sécurité qui exécute la procédure de Modification de Clé de Session. La Figure 7 représente en détail les messages et les données échangés.

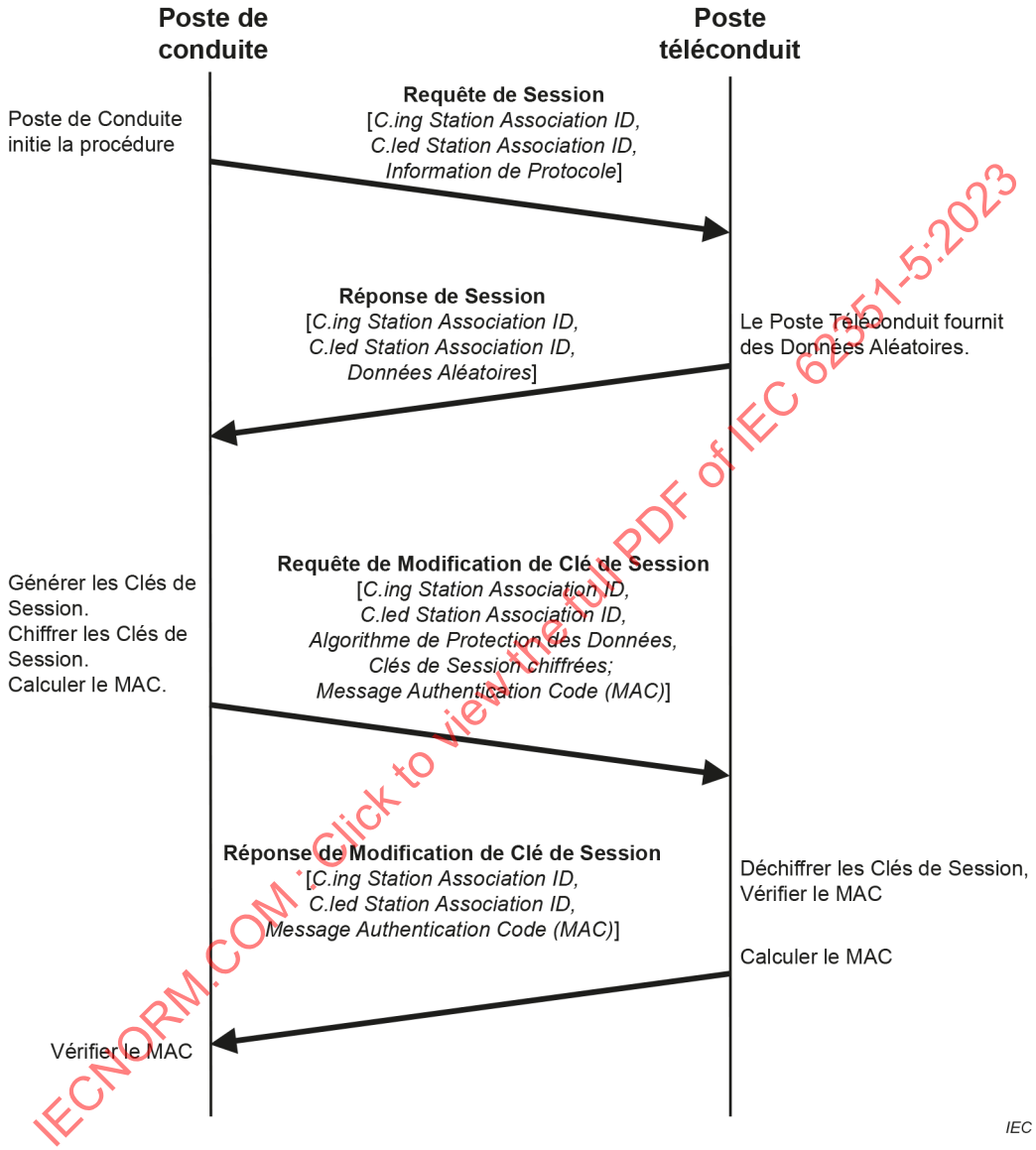


Figure 7 – Procédure de Modification de Clé de Session

8.4.2.2 Message de Requête de Session

8.4.2.2.1 Structure

Chaque message de Requête de Session doit contenir les informations décrites en 8.4.2.2 et résumées dans le Tableau 18.

Le poste de conduite (uniquement) doit envoyer le message de Requête de Session. Par ce message, le poste de conduite initie la procédure de Modification de Clé de Session. Le message de Requête de Session doit entraîner un message de Réponse de Session de la part du poste téléconduit.

Après l'envoi du message de Requête de Session, le poste de conduite doit enclencher l'Horloge de Réponse afin de vérifier que le message de Réponse de Session du poste téléconduit est reçu dans le délai prévu. Si l'Horloge de Réponse expire (Temporisation de Réponse), le poste de conduite doit exécuter les actions indiquées dans le diagramme d'état correspondant décrit en 8.4.3.

Tableau 18 – Message de Requête de Session

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur Valeur	PRI = Information de protocole

Valeur	CGL = Contrôle de la longueur des données aléatoires de la station
Nombre d'octets spécifié dans CGL	CGD = Contrôle des données aléatoires de la station

8.4.2.2.2 ID d'Association du poste de conduite

Il s'agit de la valeur que le poste de conduite a choisie pour représenter la liaison de communication avec ce poste téléconduit. Cette valeur doit correspondre à l'AIM dans la dernière Requête de Modification de Clé de Mise à Jour envoyée au poste téléconduit pendant la procédure d'Association de Poste réussie réalisée le plus récemment pour cette liaison de communication, comme cela est décrit en 8.3.5.4.

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

8.4.2.2.3 ID d'Association du poste téléconduit

Il s'agit de la valeur que le poste téléconduit a choisie pour représenter la liaison de communication avec ce poste de conduite. Cette valeur doit correspondre à l'AIS dans la dernière Réponse de Modification de Clé de Mise à Jour reçue du poste téléconduit pendant la procédure d'Association de Poste réussie réalisée le plus récemment pour cette liaison de communication, comme cela est décrit en 8.3.5.5.

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

8.4.2.2.4 Information de Protocole

Le poste de conduite utilise ce champ pour fournir l'information de protocole, y compris la version de protocole qu'il a l'intention d'utiliser avec le poste téléconduit.

La structure et les valeurs possibles dans ce champ doivent être spécifiées par les normes de référence du protocole concerné.

Le poste de conduite et le poste téléconduit peuvent prendre en charge de multiples versions de protocole. Le poste téléconduit doit valider la valeur d'Information de Protocole spécifiée dans le message de Requête de Session reçu. Les règles de validation de cette valeur sur le poste téléconduit doivent être spécifiées dans les normes de référence du protocole concerné.

S'il est considéré que la valeur d'Information de Protocole n'est pas valide dans la norme de référence, le poste téléconduit doit ignorer la Requête de Session qu'il a reçue.

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

8.4.2.2.5 Longueur des données aléatoires de la station de contrôle

Cette valeur doit spécifier la longueur en octets des données aléatoires qui suivent. La longueur minimale des données aléatoires dans ce message doit être de quatre octets, la longueur maximale est de 64 octets.

CGL:= UI8[1..8]<4..64>

8.4.2.2.6 Contrôle des données aléatoires de la station

La station de contrôle doit inclure ces données aléatoires dans le message de demande de session pour s'assurer que le contenu du message de réponse de session ultérieur n'est pas prévisible et pour protéger la station de contrôle contre les attaques par répétition. Les données aléatoires doivent être générées à l'aide de l'algorithme spécifié dans NIST SP 800-90A Rev.1.

CGD:= OS8i[1..8i]; i:=CGL

8.4.2.3 Message de Réponse de Session

8.4.2.3.1 Structure

Chaque message de Réponse de Session doit contenir les informations décrites en 8.4.2.3 et résumées dans le Tableau 19.

Le poste téléconduit (seulement) doit envoyer le message de Réponse de Session chaque fois qu'un message de Requête de Session est reçu du poste de conduite.

La Réponse de Session fournit des données aléatoires que le poste de conduite doit utiliser pour authentifier le message de Requête de Modification de Clé de Session suivant.

Après l'envoi du message de Réponse de Session, le poste téléconduit doit enclencher l'Horloge de Requête afin de vérifier que le message de Requête de Modification de Clé de Session du poste de conduite qui suit est reçu dans le délai prévu. Si l'Horloge de Requête expire (Temporisation de Requête), le poste téléconduit doit exécuter les actions indiquées dans le diagramme d'état correspondant décrit en 8.4.4.

L'Horloge de Requête doit être arrêtée lorsqu'un message de Requête de Modification de Clé de Session valide est reçu..

Tableau 19 – Message de Réponse de Session

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur	CGL = Longueur de données aléatoires du poste téléconduit
Nombre d'octets spécifié dans la CGD	CGD = Données aléatoires du poste téléconduit
Nombre d'octets spécifiés par l'algorithme MAC (MAL) sélectionné dans le message Update Key Change Request, défini dans 8.3.5.4.5	MAC = Code d'authentification du message

8.4.2.3.2 ID d'Association du poste de conduite

Cette valeur doit correspondre à l'AIM dans le message de Requête de Session reçu le plus récemment du poste de conduite, décrit en 8.4.2.2.2.

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

8.4.2.3.3 ID d'Association du poste téléconduit

Cette valeur doit correspondre à l'AIS dans le message de Requête de Session reçu le plus récemment du poste de conduite, décrit en 8.4.2.2.3.

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

8.4.2.3.4 Longueur de Données Aléatoires du poste téléconduit

Cette valeur doit spécifier la longueur en octets des données aléatoires qui suivent. La longueur minimale des données aléatoires dans ce message doit être de quatre octets, la longueur maximale est de 64 octets.

CGL:= UI8[1..8]<4..64>

8.4.2.3.5 Données Aléatoires du poste téléconduit

Le poste téléconduit doit inclure ces données aléatoires dans le message de Réponse de Session afin d'assurer que le contenu du message de Requête de Modification de Clé de Session qui suit n'est pas prévisible, et de protéger le poste téléconduit contre les attaques par rejeu.

Les générateurs de nombres aléatoires sont chargés de fournir des données aléatoires statistiquement adéquates. Des conseils pour la génération de nombres aléatoires peuvent être trouvés dans NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C ainsi que dans IETF RFC 4086

CGD:= OS8i[1..8i]; i:=CGL

8.4.2.3.6 Code d'authentification des messages

La station contrôlée doit utiliser ce champ pour authentifier les données incluses dans le message de réponse de session transmis.

Cette valeur doit être calculée à l'aide de l'algorithme MAC sélectionné dans le message de demande de changement de clé de mise à jour, décrit au 8.3.5.4.5, en utilisant la clé de mise à jour d'authentification correspondante générée comme décrit au 8.3.10.

La station de contrôle doit transmettre les données via l'algorithme MAC dans l'ordre décrit dans le Tableau 20, les normes de référence peuvent nécessiter des informations supplémentaires, en plus de celles indiquées dans le Tableau 20, , à inclure dans le calcul MAC. La longueur de la valeur MAC résultante, en fonction de l'algorithme MAC sélectionné, doit être tronquée comme indiqué au 8.3.5.4.5.

Tableau 20 – Données incluses dans le calcul MAC (dans l'ordre)

Données	Description	Décrit dans	Source
Valeurs de demande de session	L'intégralité du message de demande de session reçu le plus récemment.	Paragraphe 8.4.2.2	Demande de session
Réponse de session valeurs	L'ensemble du message de réponse de session transmis jusqu'à et y compris CGD (à l'exclusion du champ MAC).	Paragraphe 8.4.2.3	Réponse de session
Données de bourrage	Données de bourrage supplémentaires requises par l'algorithme MAC.	Spécification de l'algorithme	Requis par l'algorithme

MAC:= OS8i[1..8i]; i:= comme spécifié dans MAL de ce message, défini au 8.3.5.4.5.

8.4.2.4 Message de Requête de Modification de Clé de Session

8.4.2.4.1 Structure

Chaque message de Requête de Modification de Clé de Session doit contenir les informations décrites en 8.4.2.4 et résumées dans le Tableau 20.

Seul le poste de conduite doit envoyer des messages de Requête de Modification de Clé de Session. Un message de Requête de Modification de Clé de Session doit être une notification envoyée par le poste de conduite d'une modification des Clés de Session et doit entraîner un message de Réponse de Modification de Clé de Session du poste téléconduit.

Après l'envoi du message de Requête de Modification de Clé de Session, le poste de conduite doit enclencher l'Horloge de Réponse afin de vérifier que le message de Réponse de Modification de Clé de Session du poste téléconduit est reçu dans le délai prévu. Si l'Horloge de Réponse expire (Temporisation de Réponse), le poste de conduite doit exécuter les actions indiquées dans le diagramme d'état décrit en 8.4.3.

Tableau 21 – Message de Requête de Modification de Clé de Session

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Valeur énumérée	DPA = Algorithme de Protection des Données
Valeur Valeur	WKL = Longueur de Données de Clé Enveloppée
Nombre d'octets spécifié dans la WKL	WKD = Données de Clé Enveloppée
Nombre d'octets spécifié par l'algorithme de MAC (MAL) choisi dans le message de Requête de Modification de Clé de Mise à Jour, décrit en 8.3.5.4.5	MAC = Code d'authentification de message

8.4.2.4.2 ID d'Association du poste de conduite

C'est la valeur que le poste de conduite a choisi de représenter la liaison de communication avec ce poste téléconduit. Cette valeur doit correspondre à l'AIM fournie dans la Requête de Session transmise le plus récemment au poste téléconduit, décrite en 8.4.2.2.2.

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

8.4.2.4.3 ID d'Association du poste téléconduit

Il s'agit de la valeur que le poste téléconduit a choisie pour représenter la liaison de communication avec ce poste de conduite. Cette valeur doit correspondre à l'AIS fournie dans la Requête de Session transmise le plus récemment au poste téléconduit, décrite en 8.4.2.2.3.

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

8.4.2.4.4 Algorithme de Protection des Données

En utilisation cette valeur, le poste de conduite doit indiquer au poste téléconduit l'algorithme choisi pour chiffrer ou authentifier les données d'application dans les messages des Données Sécurisées échangés, décrits en 8.5, après qu'il a été mis fin avec succès à la procédure de Modification de Clé de Session en cours.

Les algorithmes de chiffrement et d'authentification dont la prise en charge est obligatoire sont énumérés à l'Article 9. Exigences d'Interopérabilité. Il convient de choisir la meilleure option disponible dans ce champ.

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

<0>:= réservé

<1>:= réservé

<2>:= devenu obsolète

<3>:= HMAC-SHA-256 tronqué à 8 octets (en série)

<4>:= HMAC-SHA-256 tronqué à 16 octets (en réseau)

<5>:= devenu obsolète

<6>:= devenu obsolète

<7>:= HMAC-SHA3-256 tronqué à 8 octets (en série)

<8>:= HMAC-SHA3-256 tronqué à 16 octets (en réseau)

<9>:= BLAKE2s-256 tronqué à 8 octets (en série)

<10>:= BLAKE2s-256 tronqué à 16 octets (en réseau)

<11>:= chiffrement AEAD-AES-256-GCM (en série et en réseau)

<12..127>:= réservé pour utilisation ultérieure

<128..255>:= réservé pour les choix spécifiques au fournisseur. Interopérabilité non garantie.

8.4.2.4.5 Longueur de Données de Clé Enveloppée

Cette valeur doit être la longueur des données produites par l'algorithme d'enveloppement de clé, comme cela est décrit en 8.4.2.4.6. Noter que l'algorithme AES-256 qui sert à envelopper les Clés de Session génère au minimum une sortie de 64 octets avec une longueur de clés de session de 256 bits.

WKL:= UI16[1..16]<64 ..65535>

8.4.2.4.6 Données de Clé Enveloppée

Le poste de conduite doit utiliser cette valeur pour fournir les Clés de Session au poste téléconduit.

Cette valeur doit être obtenue par exécution de l'algorithme d'enveloppement de clé choisi lors de la dernière procédure d'Association de Poste réalisée avec succès pour cette Association, décrit en 8.3.5.4.4, à l'aide de la Clé de Mise à Jour de Chiffrement correspondante, générée comme cela est décrit en 8.3.10.

Le poste de conduite doit faire passer les données par l'Algorithme d'Enveloppement de Clé dans l'ordre décrit dans le Tableau 21.

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

Tableau 22 – Données incluses dans les WKD (dans cet ordre)

Données	Description	Décrites au	Source
Clé de Session de Direction conduite	Clé utilisée pour authentifier les données du poste de conduite.	Tableau 2	Générée par le poste de conduite
Clé de Session de Direction surveillance	Clé utilisée pour authentifier les données du poste téléconduit.	Tableau 2	Générée par le poste de conduite
Données de remplissage	Comme cela est exigé par l'algorithme d'enveloppement de clé.	Spécification de l'algorithme.	Exigé par l'algorithme.

La longueur des clés de session doit être de 256 bits (32 octets).) parce que l'algorithme sélectionné dans le champ DPA du message Demande de changement de clé de session, décrit au 8.4.2.4.4, nécessite une clé de 256 bits. Les générateurs de clé de session sont chargés de fournir des données aléatoires statistiquement adéquates. Des conseils pour la génération de nombres aléatoires peuvent être trouvés dans NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C ainsi que dans IETF RFC 4086.

Les Clés de Session doivent être traitées comme des tableaux d'octets et transmises en commençant par l'octet dont l'indice est le plus bas. Par exemple, l'Annexe A de la spécification AES FIPS PUB 197 fournit l'exemple d'une clé chiffrée de 256 bits présentée dans le Tableau 22. Le bit d'indice 0, de valeur 2B, doit être transmis le premier, comme cela est indiqué dans le Tableau 22.

Tableau 23 – Exemple d'ordre de Clé de Session

Valeur	60	3D	EB	10	15	CA	71	BE	2B	73	AE	F0		14	DF	F4
Indice	0	1	2	3	4	5	6	7	8	9	10	11		29	30	31
NOTE La sortie de l'algorithme d'enveloppement de clé peut être plus longue que l'entrée. Par exemple, l'Algorithme d'Enveloppement de Clé AES produit une sortie qui est plus longue d'exactement 8 octets que son entrée.																

8.4.2.4.7 Code d'Authentification de Message

Le poste de conduite doit utiliser cette valeur pour authentifier les données incluses dans le message de Requête de Modification de Clé de Session en transmission.

Cette valeur doit être calculée au moyen de l'algorithme de MAC choisi lors de la dernière procédure d'Association de Poste réalisée avec succès pour cette liaison de communication, décrite en 8.3.5.3.5, à l'aide de la Clé de Mise à Jour de Chiffrement correspondante, générée comme cela est décrit en 8.3.10.

Le poste de conduite doit faire passer les données par l'algorithme de MAC dans l'ordre décrit dans le Tableau 23, , les normes de référence peuvent nécessiter des informations supplémentaires, en plus de celles indiquées dans le Tableau 23 à inclure dans le calcul MAC. La longueur de la valeur de MAC résultante, en fonction de l'algorithme de MAC choisi, doit être tronquée comme cela est indiqué en 8.3.5.3.5.

Tableau 24 – Données incluses dans le calcul de MAC (dans cet ordre)

Données	Description	Décrites au	Source
Données Aléatoires du poste téléconduit	Les données aléatoires fournies dans la Réponse de Session reçue le plus récemment de la part du poste téléconduit.	Paragraphe 8.4.2.3.5	Réponse de Session
Valeurs de Requête de Modification de Clé de Session	L'intégralité du message de Requête de Modification de Clé de Session en transmission jusqu'aux WKD compris (à l'exclusion du champ MAC).	Paragraphe 8.4.2.4	Requête de Modification de Clé de Session
Données de remplissage	Comme cela est exigé par l'algorithme de MAC.	Spécification de l'algorithme.	Exigé par l'algorithme.

MAC:= OS8i[1..8i]; i:=comme cela est spécifié dans le MAL du message de Requête de Modification de Clé de Mise à Jour reçu le plus récemment, décrit en 8.3.5.3.5.

8.4.2.5 Message de Réponse de Modification de Clé de Session

8.4.2.5.1 Structure

Chaque message de Réponse de Modification de Clé de Session doit contenir les informations décrites en 8.4.2.4 et résumées dans le Tableau 24.

Le poste téléconduit (seulement) doit envoyer les messages de Réponse de Modification de Clé de Session chaque fois qu'un message valide de Requête de Modification de Clé de Session est reçu du poste de conduite. Par ce message, le poste téléconduit confirme au poste de conduite la possession des nouvelles clés de Session et conclut la procédure de Modification de Clé de Session.

Tableau 25 – Message de Réponse de Modification de Clé de Session

Valeur Valeur	AIM = ID d'Association du Poste de Conduite
Valeur Valeur	AIS = ID d'Association du Poste téléconduit
Nombre d'octets spécifié par l'algorithme de MAC (MAL) choisi dans le message de Requête de Modification de Clé de Mise à Jour, décrit en 8.3.5.4.5	MAC = Code d'authentification de message

8.4.2.5.2 ID d'Association du poste de conduite

Cette valeur doit correspondre à l'AIM dans le message de Requête de Modification de Clé de Session reçu le plus récemment du poste de conduite, décrit en 8.4.2.4.2.

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

8.4.2.5.3 ID d'Association du poste téléconduit

Cette valeur doit correspondre à l'AIS dans le message de Requête de Modification de Clé de Session reçu le plus récemment du poste de conduite, décrit en 8.4.2.4.3.

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

8.4.2.5.4 Code d'Authentification de Message

Le poste téléconduit doit utiliser cette valeur pour authentifier les données incluses dans le message de Réponse de Modification de Clé de Session en transmission.

Cette valeur doit être calculée au moyen de l'algorithme de MAC choisi lors de la dernière procédure d'Association de Poste réalisée avec succès pour cette Association, décrite en 8.3.5.4.5, à l'aide de la Clé de Mise à Jour d'Authentification correspondante, générée comme cela est décrit en 8.3.10.

Le poste de conduite doit faire passer les données par l'algorithme de MAC dans l'ordre décrit dans le Tableau 26, les normes de référence peuvent nécessiter des informations supplémentaires, en plus de celles indiquées dans le Tableau 26, à inclure dans le calcul du MAC. La longueur de la valeur de MAC résultante, en fonction de l'algorithme de MAC choisi, doit être tronquée comme cela est indiqué en 8.3.5.4.5.

Tableau 26 – Données incluses dans le calcul de MAC (dans cet ordre)

Données	Description	Décrites au	Source
Valeurs de Requête de Modification de Clé de Session	L'intégralité du message de Requête de Modification de Clé de Session reçu le plus récemment du poste de conduite.	Paragraphe 8.4.2.4	Requête de Modification de Clé de Session
Valeurs de Réponse de Modification de Clé de Session	L'intégralité du message de Réponse de Modification de Clé de Session en transmission jusqu'à l'AIS compris (à l'exclusion du champ MAC).	Paragraphe 8.4.2.5	Réponse de Modification de Clé de Session
Données de remplissage	Comme cela est exigé par l'algorithme de MAC.	Spécification de l'algorithme.	Exigé par l'algorithme.

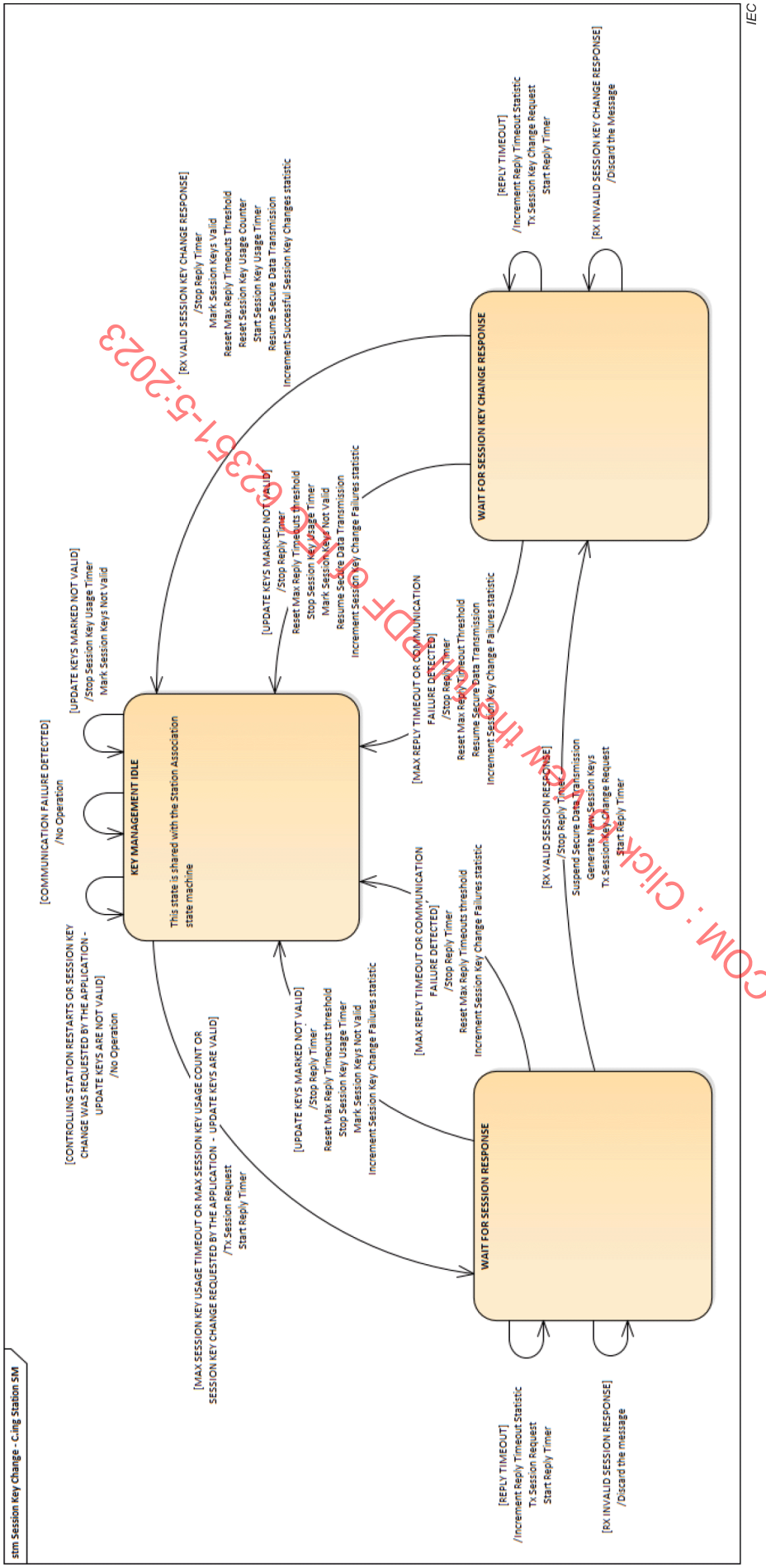
MAC:= OS8i[1..8i]; i:=comme cela est spécifié dans le MAL du message de Requête de Modification de Clé de Mise à Jour reçu le plus récemment, défini en 8.3.5.4.5.

8.4.2.6 Procédure de Modification de Clé de Session sollicitée par le poste téléconduit

Si des messages non sollicités spontanés en provenance du poste téléconduit sont admis, ce dernier peut, de manière facultative, solliciter le poste de conduite pour qu'il initie la procédure de Modification de Clé de Session par l'envoi d'un message de Requête d'Initiation de Session. Les normes de référence du protocole concerné peuvent définir le message de Requête d'Initiation de Session et sa gestion.

8.4.3 Diagramme d'état du poste de conduite

Sur le poste de conduite, les messages de Modification de Clé de Session décrits en 8.4.2 doivent être gérés par le diagramme d'état décrit en 8.4.3. La Figure 8 représente les transactions de Modification de Clé de Session sur le poste de conduite. Le poste de conduite doit exécuter le diagramme d'état Modification de Clé de Session décrit dans le Tableau 27. L'état *Inactif de Gestion de Clés* est partagé (en commun) avec le diagramme d'état d'Association de Poste.



Anglais	Français
COMMUNICATION FAILURE DETECTED/ No Operation	ÉCHEC DE COMMUNICATION DÉTECTÉ/ Pas d'Opération
CONTROLLING STATION RESTARTS OR SESSION KEY CHANGE WAS REQUESTED BY THE APPLICATION – UPDATE KEYS ARE NOT VALID	LE POSTE DE CONDUITE REDÉMARRE OU LA MODIFICATION DES CLÉS DE SESSION A ÉTÉ DEMANDÉE PAR L'APPLICATION – LES CLÉS DE MISE À JOUR NE SONT PAS VALIDES
UPDATE KEYS MARKED NOT VALID	CLÉS DE MISE À JOUR MARQUÉES NON VALIDES
Stop Session Key Usage Timer; Mark Session Keys Not Valid	Arrêter l'Horloge d'Utilisation de Clé de Session; Marquer les Clés de Session comme Non Valides
KEY MANAGEMENT IDLE	ÉTAT INACTIF DE GESTION DE CLÉS
This state is shared with the Station Association state machine	Cet état est partagé avec le diagramme d'état Association de Poste
MAX SESSION KEY USAGE TIMEOUT OR MAX SESSION KEY USAGE COUNT OR SESSION KEY CHANGE REQUESTED BY THE APPLICATION – UPDATE KEYS ARE VALID; Tx Session Request; Start Reply Timer	TEMPORISATION DU NOMBRE MAXIMAL D'UTILISATIONS DE CLÉ DE SESSION OU COMPTE MAXIMAL D'UTILISATION DE CLÉ DE SESSION OU MODIFICATION DE CLÉS DE SESSION DEMANDÉE PAR L'APPLICATION – LES CLÉS DE MISE À JOUR SONT VALIDES; Requête de Session Tx; Enclencher l'Horloge de Réponse
Stop Reply Timer	Arrêter l'Horloge de Réponse
Reset Max Reply Timeout Threshold	Réinitialiser le seuil du Nombre maximal de temporisations de réponse
Stop Session Key Usage Timer	Arrêter l'Horloge d'Utilisation de Clé de Session
Increment Session Key Change Failures statistic	Incrémenter la statistique Échecs de Modification de Clés de Session
Resume Secure Data Transmission	Reprendre la Transmission des Données Sécurisées
Rx VALID SESSION KEY CHANGE RESPONSE	RÉPONSE DE MODIFICATION DE CLÉS DE SESSION VALIDE RX
Mark Session Keys Valid	Marquer les Clés de Session comme Valides
Reset Session Key Usage Counter	Réinitialiser le Compteur d'Utilisation de Clé de Session
Start Session Key Usage Timer	Enclencher l'Horloge d'Utilisation de Clé de Session
Increment Successful Session Key Changes statistic	Incrémenter la statistique Modifications Réussies de Clés de Session
MAX REPLY TIMEOUT OR COMMUNICATION FAILURE DETECTED	TEMPORISATION DU NOMBRE MAXIMAL DE RÉPONSES OU ÉCHEC DE COMMUNICATION DÉTECTÉ
REPLY TIMEOUT	TEMPORISATION DE RÉPONSE
Increment Reply Timeout statistic	Incrémenter la statistique Temporisation de Réponse
WAIT FOR SESSION RESPONSE	ATTENDRE LA RÉPONSE DE SESSION
Rx VALID SESSION RESPONSE	RÉPONSE DE SESSION VALIDE Rx
Suspend Secure Data Transmission	Interrompre la Transmission des Données Sécurisées

Generate New Session Keys	Générer de nouvelles Clés de Session
Tx Session Key Change Request	Requête de Modification de Clés de Session Tx
WAIT FOR SESSION KEY CHANGE RESPONSE	ATTENDRE LA RÉPONSE DE MODIFICATION DE CLÉS DE SESSION
Rx INVALID SESSION KEY CHANGE RESPONSE	RÉPONSE DE MODIFICATION DE CLÉS DE SESSION NON VALIDE RX
Discard the message	Ignorer le message
Rx INVALID SESSION RESPONSE	RÉPONSE DE SESSION NON VALIDE Rx

Figure 8 – Modification de Clé de Session – Diagramme d'état du poste de conduite

Tableau 27 – Diagramme d'état du poste de conduite: Modification de Clé de Session

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Association de Poste)		**Attendre la Réponse de Session**		**Attendre la Réponse de Modification de Clé de Session**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse au message de Requête de Session		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Session.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Expiration du Temps d'Utilisation de Clé de Session	Le Temps d'Utilisation de Clé de Session a expiré.	Transmettre le message de Requête de Session. Enclencher l'Horloge de Réponse.	Attendre la Réponse de Session	Pas d'Opération. (Cet événement doit être géré dans l'état "*Inactif de Gestion de Clés*")	Attendre la Réponse de Session	Pas d'Opération. (Cet événement doit être géré dans l'état "Inactif de Gestion de Clés")	Attendre la Réponse de Modification de Clé de Session	**1**
Dépassement du Compte d'Utilisation de Clé de Session	Le nombre d'utilisations de la clé de session a dépassé le seuil de Compte maximal d'Utilisation de Clé de Session.	Transmettre le message de Requête de Session. Enclencher l'Horloge de Réponse.	Attendre la Réponse de Session	Pas d'Opération. (Cette condition doit être vérifiée lorsque le diagramme d'état est dans l'état "*Inactif de Gestion de Clés*")	Attendre la Réponse de Session	Pas d'Opération. (Cette condition doit être vérifiée lorsque le diagramme d'état est dans l'état "*Inactif de Gestion de Clés*")	Attendre la Réponse de Modification de Clé de Session	**2**

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Association de Poste)		**Attendre la Réponse de Session**		**Attendre la Réponse de Modification de Clé de Session**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse au message de Requête de Session		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Session.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Modification de Clé de Session demandée par l'application	L'application a demandé d'exécuter la procédure de Modification de Clé de Session.	SI les Clés de Mise à Jour sont Valides: Transmettre le message de Requête de Session. Enclencher l'Horloge de Réponse.	Attendre la Réponse de Session	Ignorer l'événement. (Le poste de conduite exécute déjà la procédure dans cet état)	Attendre la Réponse de Session	Ignorer l'événement. (Le poste de conduite exécute déjà la procédure dans cet état)	Attendre la Réponse de Modification de Clé de Session	3
		SI les Clés de Mise à Jour Ne sont Pas Valides: Pas d'Opération.	État Inactif de Gestion de Clés					
Réponse de Session Valide Rx	Le poste de conduite a reçu une Réponse de Session avec des paramètres valides.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Arrêter l'Horloge de réponse Interrompre la transmission de données sécurisées dans le diagramme d'état Échange de Données Sécurisées Générer les nouvelles Clés de Session Transmettre le message de Requête de Modification de Clé de Session. Enclencher l'Horloge de Réponse.	Attendre la Réponse de Modification de Clé de Session	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Session	4

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés **(cet état est partagé avec le diagramme d'état Association de Poste)**		**Attendre la Réponse de Session**		**Attendre la Réponse de Modification de Clé de Session**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse au message de Requête de Session		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Session.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse de Session Non Valide Rx: le message n'est pas authentique.	Le poste de conduite a reçu un message de réponse de session avec des informations d'authentification non valides.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Incrémenter la statistique Erreurs d'authentification de clé. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Session	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Session	**5**

Événement	Description de l'événement	État						
		État Inactif de Gestion de Clés (cet état est partagé avec le diagramme d'état Association de Poste)		**Attendre la Réponse de Session**		**Attendre la Réponse de Modification de Clé de Session**		
		État stable pour la gestion des Clés de Session et des Clés de Mise à Jour		Le poste de conduite attend que le poste téléconduit envoie la réponse au message de Requête de Session		Le poste de conduite attend que le poste téléconduit envoie la réponse à la Requête de Modification de Clé de Session.		
		Action	**État Suivant**	**Action**	**État Suivant**	**Action**	**État Suivant**	
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
Réponse de Modification de Clé de Session Non Valide Rx: Le message contient des erreurs de paramètres.	Le poste de conduite a reçu un message de Session avec avec l'une des conditions d'erreur suivantes : a) L'ID d'association de la station de contrôle ne correspond pas à celui de la demande de session b) L'ID d'association de la station contrôlée ne correspond pas à celui de la demande de session c) La longueur des données aléatoires est inférieure au minimum requis d) La longueur des données aléatoires dépasse le maximum autorisé.	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	État Inactif de Gestion de Clés	Incrémenter la statistique *Messages Inattendus*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Session	Incrémenter la statistique *Erreurs d'Authentification des Clés*. Ignorer le message. Incrémenter la statistique *Messages Ignorés*.	Attendre la Réponse de Modification de Clé de Session	**6**