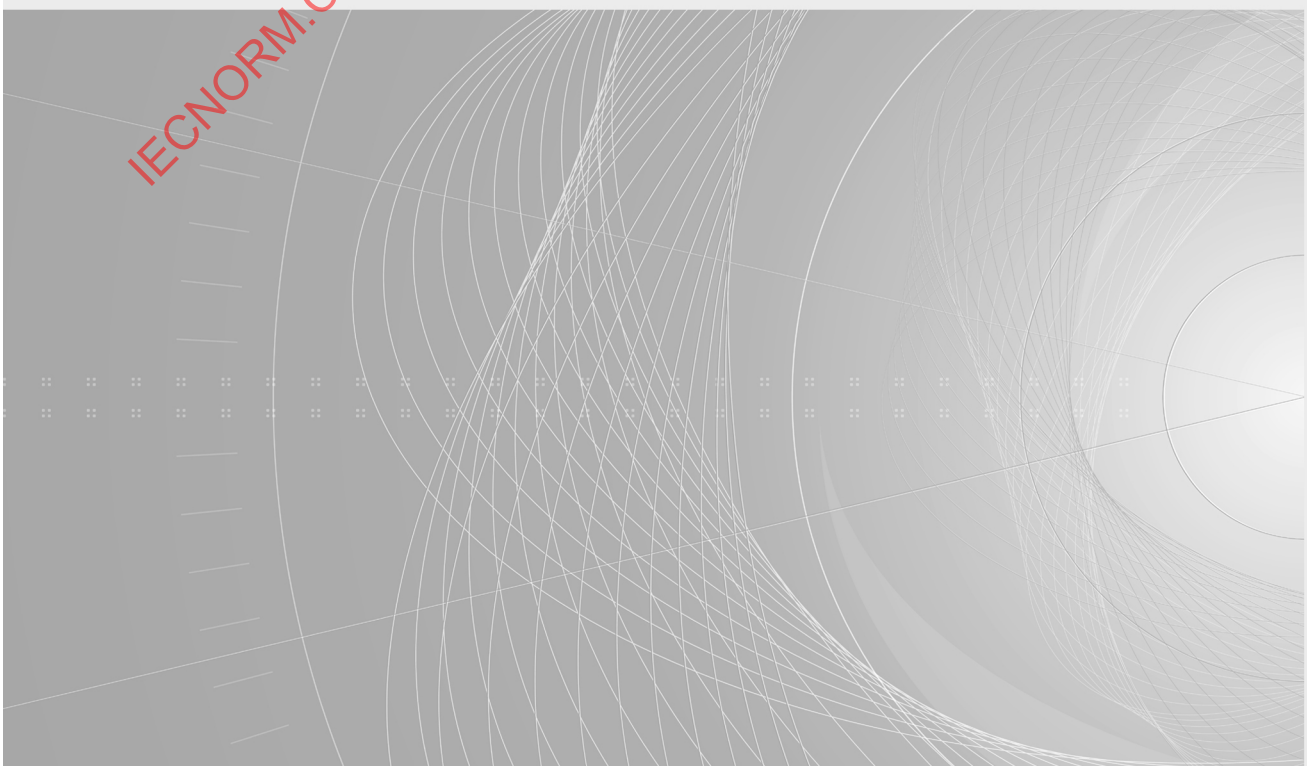
IEC/TS 60870-5-7

Edition 1.0 2013-07

TECHNICAL SPECIFICATION

colour inside

Telecontrol equipment and systems – Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)



IEC/TS 60870-5-7:2013(E)

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

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

IEC/TS 60870-5-7

Edition 1.0 2013-07

TECHNICAL SPECIFICATION

Telecontrol equipment and systems – Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-0919-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

IEC 60870-5-7, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/1308/DTS	57/1339/RVC

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

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

In this publication the following print types are used:

Clause 10: Direct quotations from IEC/TS 62351-3:2007: in italic type.

A list of all the parts in the IEC 60870 series, published under the general title *Telecontrol equipment and systems*, can be found on the IEC website.

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

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

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

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

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

1 Scope

This part of IEC 60870 describes messages and data formats for implementing IEC/TS 62351-5 for secure authentication as an extension to IEC 60870-5-101 and IEC 60870-5-104.

The purpose of this base standard is to permit the receiver of any IEC 60870-5-101/104 Application Protocol Data Unit (APDU) to verify that the APDU was transmitted by an authorized user and that the APDU was not modified in transit. It provides methods to authenticate not only the device which originated the APDU but also the individual human user if that capability is supported by the rest of the telecontrol system.

This specification is also intended to be used, together with the definitions of IEC/TS 62351-3, in conjunction with the IEC 60870-5-104 companion standard.

The state machines, message sequences, and procedures for exchanging these messages are defined in the IEC/TS 62351-5 specification. This base standard describes only the message formats, selected options, critical operations, addressing considerations and other adaptations required to implement IEC/TS 62351 in the IEC 60870-5-101 and 104 protocols.

The scope of this specification does not include security for IEC 60870-5-102 or IEC 60870-5-103. IEC 60870-5-102 is in limited use only and will therefore not be addressed. Users of IEC 60870-5-103 desiring a secure solution should implement IEC 61850 using the security measures from in IEC/TS 62351 referenced in IEC 61850.

Management of keys, certificates or other cryptographic credentials within devices or on communication links other than IEC 60870-5-101/104 is out of the scope of this specification and may be addressed by other IEC/TS 62351 specifications in the future.

2 Normative references

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

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

IEC 60870-5-104:2006, *Telecontrol equipment and systems – Part 5-104:Transmission protocols – Network access for IEC 60870-5-101 – Using standard transport profiles*

IEC/TS 62351-3:2007, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC/TS 62351-5:2013, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

NOTE Terms 3.1.1 to 3.1. 7 are included here because they are specific to the IEC 60870-5 standards and may be useful for reading this specification as an independent document. Terms 3.1.8 to 3.1.9 are included here because they are specific to IEC/TS 62351-5.

3.1.1
Application Protocol Data Unit
complete application layer message transmitted by a station

3.1.2
Application Service Data Unit
application layer message submitted to lower layers for transmission

3.1.3
Controlling Station
device or application that initiates most of the communications and issues commands

Note 1 to entry: Commonly called a “master” in some protocol specifications.

3.1.4
Controlled Station
remote device that transmits data gathered in the field to the controlling station

Note 1 to entry: Commonly called the “outstation” or “slave” in some protocols.

3.1.5
Control Direction
data transmitted by the controlling station to the controlled station(s)

3.1.6
Message Authentication Code
calculated value used by a receiving station to authenticate and check the integrity of an Application Protocol Data Unit

3.1.7
Monitoring Direction
data transmitted by the controlled station to the controlling stations

3.1.8
Challenger
station that issues authentication challenges. May be either a controlled or controlling station.

3.1.9
Responder
station that responds or reacts to authentication challenges. May be either a controlled or controlling station.

3.2 Abbreviated terms

Refer to IEC/TS 62351-2 for a list of applicable abbreviated terms. Terms 3.2.1 to 3.2.3 are included here because they are specifically used in the affected protocols and used in the discussion of this authentication mechanism.

3.2.1
ASDU
Application Service Data Unit

3.2.2
APDU
Application Protocol Data Unit

3.2.3
MAC
Message Authentication Code

4 Selected options

4.1 Overview of clause

This clause describes which of the options specified in IEC/TS 62351-5 shall be implemented in IEC 60870-5-101 and IEC 60870-5-104.

4.2 MAC algorithms

IEC 60870-5 stations shall implement all the mandatory MAC algorithms listed in IEC/TS 62351-5, and may implement any of the optional MAC algorithms listed there.

4.3 Encryption algorithms

IEC 60870-5 stations shall implement all the mandatory encryption algorithms listed in IEC/TS 62351-5, and may implement any of the optional encryption algorithms listed there.

4.4 Maximum error count

IEC 60870-5 stations may implement a maximum error count in the range specified in IEC/TS 62351-5.

4.5 Use of aggressive mode

IEC 60870-5 stations shall implement IEC/TS 62351-5 aggressive mode. Aggressive mode shall be the normal method of authentication for stations implementing this specification. However, IEC 60870-5 stations shall also permit it to be configured as disabled. A station with aggressive mode disabled shall not transmit any S_AR_NA_1 Aggressive Mode Request ASDUs and shall reply to any such ASDUs with S_ER_NA_1 Authentication Error ASDUs, subject to the limitations on Error messages described in IEC/TS 62351-5.

Regardless of whether aggressive mode is disabled, IEC 60870-5 stations shall initialize the challenge data in both directions when establishing communications, as described in 8.2.

5 Operations considered critical

IEC 60870-5-101 and IEC 60870-5-104 ASDUs identified as “M” (for “Mandatory”) in the “M/O” (“Mandatory or Optional”) column in 10.10 shall be considered critical operations. Stations complying with this standard shall require the sender to authenticate those ASDUs. Any station may optionally require authentication of any other ASDUs.

Devices complying with this standard shall provide information along with the Interoperability Tables identifying which ASDUs the device/station considers critical, requiring authentication. Refer to 10.10. If an ASDU is identified as critical, the ACT or DEACT cause of transmission is shall be considered mandatory critical, but not ACTCON or ACT_TERM.

IEC/TS 62351-5 states that any device may arbitrarily decide that an ASDU is critical and can therefore initiate a challenge for any reason. However, IEC 60870-5 shall not enforce this rule. ASDUs that are considered critical at any time by an IEC 60870-5 station shall always be considered critical by that station unless the station is reconfigured.

Any ASDUs capable of changing security configuration parameters, now or in the future, shall be considered critical.

6 Addressing information

Each IEC 60870-5-101 station shall include in its MAC calculations the destination station address from the IEC 60870-5 data link layer in the “Addressing Information” portion of the calculation. The octets of the address when included in the calculation shall be as transmitted.

7 Implementation of messages

7.1 Overview of clause

This clause describes how the secure authentication messages described in IEC/TS 62351-5 are implemented in IEC 60870-5-101 and IEC 60870-5-104.

7.2 Data definitions

7.2.1 Causes of transmission

Stations implementing secure authentication shall use the causes of transmission listed in Table 1 in addition to those described in 7.2.3 of IEC 60870-5-101:2003.

Table 1 – Additional cause of transmission

Cause := UI6[1..6]<14..16>
<14> := authentication
<15> := maintenance of authentication session key
<16> := maintenance of user role and update key

7.2.2 Type identifiers

Stations implementing secure authentication shall use the Type Identifications listed in Table 2 in addition to those described in 7.2.1 of IEC 60870-5-101:2003 and Clause 6 of IEC 60870-5-104:2006. This range of Type Identifications was previously allocated for system information in the monitor direction. The ASDUs identified by these types may be transmitted in either the control or monitor direction.

Table 2 – Additional type identifiers

TYPE IDENTIFICATION	:=	UI8[1..8]<81..87>	
<41>	:=	integrated totals containing time tagged security statistics	S_IT_TC_1
<81>	:=	authentication challenge	S_CH_NA_1
<82>	:=	authentication reply	S_RP_NA_1
<83>	:=	aggressive mode authentication request	S_AR_NA_1
<84>	:=	session key status request	S_KR_NA_1

<85>	:=	session key status	S_KS_NA_1
<86>	:=	session key change	S_KC_NA_1
<87>	:=	authentication error	S_ER_NA_1
<90>	:=	user status change	S_US_NA_1
<91>	:=	update key change request	S_UQ_NA_1
<92>	:=	update key change reply	S_UR_NA_1
<93>	:=	update key change symmetric	S_UK_NA_1
<94>	:=	update key change asymmetric	S_UA_NA_1
<95>	:=	update key change confirmation	S_UC_NA_1

7.2.3 Security statistics

Stations implementing secure authentication shall use the ASDU Type 41: *Integrated totals containing time-tagged security statistics* to report the values of the security statistics described in 7.3.2 of IEC/TS 62351-5:2013. This ASDU type is defined in 7.3.15. The Information Object Address of each security statistic shall be recorded in the Protocol Implementation Conformance Statement for each station as described in 10.9.

The procedures used by the outstation to report the security statistics shall be the same as for the existing integrated totals, as described in 7.4.8 of IEC 60870-5-101:2003, particularly including the ability for these totals to be reported using spontaneous transmission.

All security statistics shall be placed reported in a single integrated totals group.

7.2.4 Variable length data

IEC/TS 62351-5 allocates two octets in each message for the length field of variable length data, permitting the variable length data to be up to 62 335 octets long. In all cases, this is much larger than necessary. To conserve buffer space and reduce the probability of buffer overflow attacks, the maximum value of these length fields shall be limited as defined in Table 3.

Table 3 – Maximum lengths of variable length data

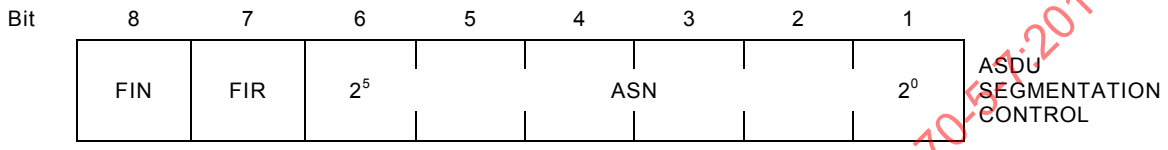
Abbrev.	Name	Subclause in IEC 60870-5-7:2013	Message name	Maximum length for IEC/TS 60870-5-7 (octets)
CLN	Challenge data length	7.3.1 7.3.4 7.3.11	Challenge Key Status Update Key Change Reply	64
HLN	MAC length	7.3.2	Reply	64
WKL	Wrapped key data length	7.3.6	Session Key Change	1 024
ELN	Error length	7.3.7	Error	128
UNL	User name length	7.3.9 7.3.10	User Status Change Update Key Change Request	256
UKL	User public key length	7.3.9	User Status Change	6 144
CDL	Certification Data Length	7.3.8	User Certificate	8 192
		7.3.9	User Status Change	1 024
CCL	Controlling station challenge data length	7.3.10	Update Key Change Request	64
EUL	Encrypted update key length	7.3.12 7.3.13	Update Key Change – sym Update Key Change – asym	8 192

7.2.5 Information object address

The Information Object Address (IOA) does not apply to the ASDUs described in IEC/TS 60870-5-7 and is not included in these ASDUs. It is replaced by the ASDU Segmentation Control octet specified in 7.2.6.

7.2.6 Transmitting extended ASDUs using segmentation

Several of the messages defined in IEC/TS 62351-5 are longer than the maximum length of an IEC 60870-5 data link or APCI frame. Figure 1 defines a field that shall be used to control reassembly when an IEC 60870-5-7 ASDU is transmitted in a series of several segments such that each segment will fit in a data link or APCI frame.



ASDU SEGMENTATION CONTROL:= CP8{FIN, FIR, ASN}

ASN := UI6[1..6]<0..63>

FIR := BS[7]<0..1>

<0> := This is not the first segment of an ASDU

<1> := This is the first segment of an ASDU

FIN := BS[8]<0..1>

<0> := This is not the final segment of an ASDU

<1> := This is the final segment of an ASDU

Figure 1 – ASDU segmentation control

If an ASDU is too long to fit in a lower-level data link or APCI frame, the excess application layer data shall be divided into segments as illustrated in Figure 2. The Data Unit Identifier fields of the ASDU(Type Id, VSQ, COT, CASDU, and ASDU SEGMENTATION CONTROL) shall be prepended to each segment so the receiving station can recognize the type, address and disposition of each segment. The station shall transmit the segments in sequence as if they were separate ASDUs, but without any data of a different Type ID interspersed.

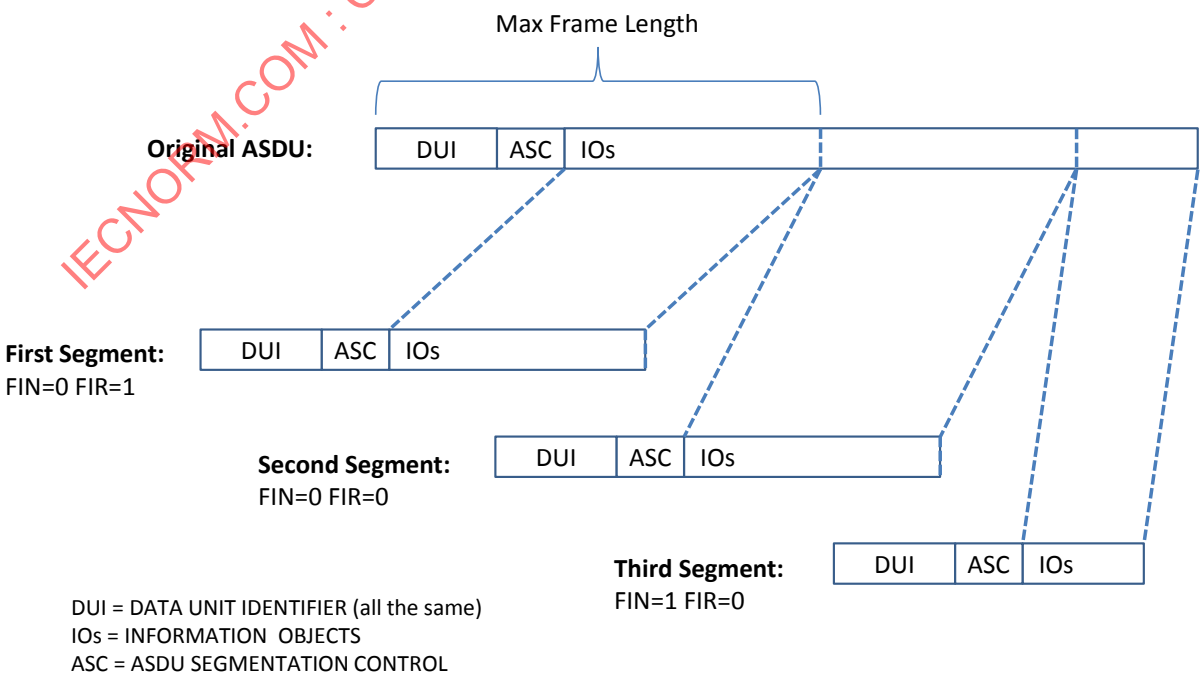


Figure 2 – Segmenting extended ASDUs

The ASN (ASDU Segment Sequence Number) shall be used to verify that segments are received in the correct order and shall help detect duplicated or missing segments. The ASN shall increment by one, modulo 64. After sequence number 63, the next sequence number value shall be 0.

The following rules shall apply when segmenting ASDUs:

1) A segment series shall begin with a segment having the FIR bit set.
2) A segment series shall end with a segment having the FIN bit set.
3) When no segment series is in progress, the receiving station shall discard any segment received without the FIR bit set.
4) A segment with the FIR bit set may have any sequence number from 0 to 63 without regard to prior history.
5) After a segment series has been started:
   a) Each subsequent segment shall have an ASN that is incremented by one (modulo 64) from the preceding segment. A received segment that meets this requirement shall become the next member of the segment series. The station shall treat all the data following the ASDU SEGMENTATION CONTROL field as if it was appended to the end of the previous data in the series.
   b) If a station receives a segment having the FIR bit set, it shall discard the entire, in-progress segment series and start a new segment series with the newly received segment as its first member.
   c) If a station receives a segment that is octet-for-octet identical to the preceding segment it shall discard the segment.
   d) If a station receives a segment having the FIR bit cleared and a sequence number other than the expected incremental number, that is not octet-for-octet identical to the preceding segment, the station shall discard the segment and the entire in-progress segment series and terminate the series.
6) A segment series may consist of a single segment having both FIR and FIN bits set.
7) When a receiving station receives a segment with the FIN bit set and therefore assembles a complete segment series, only then may the station evaluate the complete ASDU.
8) If a station receives a segment in which the Type ID, VSQ, CASDU, or COT does not match that of the first ASDU in the sequence, the station shall discard the segment and the entire series.

It is recommended that transmitting stations make each segment as large as possible for maximum efficiency of transmission. However, this is not a requirement and receiving stations shall accept varying segment lengths within the same series.

The state machine described in Table 4 defines how the station shall reassemble ASDUs from segments. This state machine assumes the reception software uses an ASDU buffer in which application data from the received segments are temporarily stored before presenting the completed ASDU to the application layer process.

There are two states:

- **Idle state**: The station is idle waiting for a segment to arrive with the FIR bit set.
- **Assembly state**: The ASDU buffer holds application data from at least one segment. While in this state, the station is awaiting additional segments to complete the ASDU.

The terminology used in Table 4 is defined as follows:

- X means “don’t care”
- SAME means the ASN is identical to the ASN in the segment immediately preceding this segment

- +1 means the ASN is incremented by one count, modulo 64, from the sequence number in the segment immediately preceding this segment
- +M, 1 < M < 64 means the sequence number is incremented by more than one count and fewer than 64 counts from the sequence number in the segment immediately preceding this segment

Table 4 – ASDU segment reception state machine

Current state	Event that triggers an action and possible transition				Action	Transition to state	
A	B			C	D	E	
If the software state is	And a segment with these fields is received			The meaning is	then perform this action	and go to this state	
	FIR	FIN	ASN				
Idle	0	X	X	Not a first segment	Discard segment.	Idle	1
	1	1	X	Entire ASDU fits within the segment	Clear the ASDU buffer, place segment's Information Object data into the ASDU buffer and pass ASDU buffer to application layer.	Idle	2
	1	0	X	First of multiple segments	Clear the ASDU buffer and place segment's Information Object data into the ASDU buffer.	Assembly	3
Assembly	0	X	SAME	IF segment is octet-for-octet identical to previous, it is a duplicate	Discard segment.	Assembly	4
	0	X	SAME	IF segment is NOT octet-for-octet identical to previous, it may be from another series	Discard segment and the entire, in-progress segment-series.	Idle	5
	0	0	+1	Expected segment received, more segments are expected	Append segment's Information Object data to contents of ASDU buffer.	Assembly	6
	0	1	+1	Expected segment received, final segment	Append segment's Information Object data to contents of ASDU buffer and pass ASDU buffer to application layer.	Idle	7
	0	X	+M 1 < M < 64	ASN is out of order	Discard segment and the entire, in-progress segment-series.	Idle	8
	1	0	X	First of multiple segments	Clear contents of ASDU buffer and place segment's Information Object data into the ASDU buffer.	Assembly	9
	1	1	X	Entire ASDU fits within the segment.	Clear contents of ASDU buffer, place segment's Information Object data into the ASDU buffer and pass ASDU buffer to Application Layer.	Idle	10
	0	X	X	IF segment is not the first of multiple segments and the Type ID, VSQ, CASDU, or COT does not match the first segment	Discard segment and the entire, in-progress segment-series.	Idle	11

Figure 3 illustrates the same state machine described in Table 4. If the two differ, Table 4 shall be considered correct.

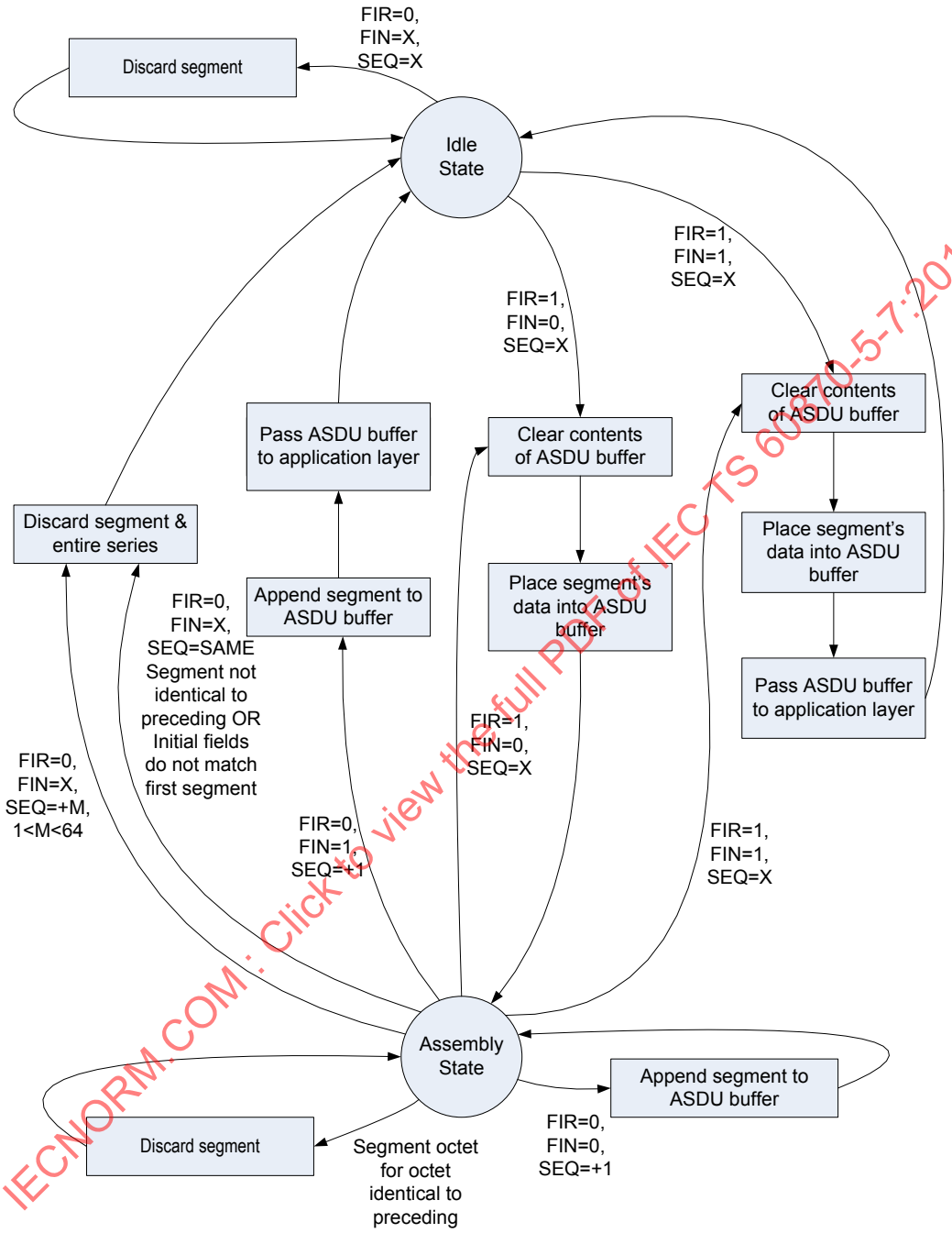


Figure 3 – Illustration of ASDU segment reception state machine

7.3 Application Service Data Units

7.3.1 TYPE IDENT 81: S_CH_NA_1 Authentication challenge

The structure of this ASDU is defined in Figure 4.

Single information object (SQ=0)

0 1 0 1 0 0 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Value	CSQ = Challenge sequence number, defined in 7.2.2.2 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User Number, defined in 7.2.2.3 of IEC/TS 62351-5:2013	
Value		
Enumerated value	MAL = MAC algorithm, defined in 7.2.2.4 of IEC/TS 62351-5:2013	
Enumerated value	RSC = Reason for challenge, defined in 7.2.2.5 of IEC/TS 62351-5:2013	
Value	CLN = Challenge data length, defined in 7.2.2.6 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in CLN	Pseudo-random challenge data, defined in 7.2.27 of IEC/TS 62351-5:2013	

Figure 4 – ASDU: S_CH_NA_1 Authentication challenge

S_CH_NA_1:= CP{Data unit identifier, CSQ, USR, HAL, RSC, CLN, Challenge Data }

CAUSES OF TRANSMISSION used with
TYPE IDENT 81:= S_CH_NA_1

CAUSE OF TRANSMISSION

In control direction:

<14>:= authentication

In monitor direction:

<14>:= authentication

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

7.3.2 TYPE IDENT 82: S_RP_NA_1 Authentication Reply

The structure of this ASDU is defined in Figure 5. In the calculation of the MAC value, the following rules apply:

a) The MAC value shall be calculated over the entire S_CH ASDU 81, not just the Information Object contained within that ASDU.

b) No lower-layer addressing information shall be included in the MAC calculation.

Single information object (SQ=0)

0 1 0 1 0 0 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Value	CSQ = Challenge sequence number, defined in 7.2.3.2 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User Number, defined in 7.2.3.3 of IEC/TS 62351-5:2013	
Value		
Value	HLN = MAC length, defined in 7.2.3.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in HLN	MAC value, defined in 7.2.3.5 of IEC/TS 62351-5:2013 and including the clarifying rules noted in this clause.	

Figure 5 – ASDU: S_RP_NA_1 Authentication Reply

S_RP_NA_1:= CP{Data unit identifier, CSQ, USR, HLN, MAC Value }

CAUSES OF TRANSMISSION used with
TYPE IDENT 82:= S_RP_NA_1

CAUSE OF TRANSMISSION

In control direction:

<14>:= authentication

In monitor direction:

<14>:= authentication

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

7.3.3 TYPE IDENT 83: S_AR_NA_1
Aggressive mode authentication request

The structure of this ASDU is defined in Figure 6.

Single information object (SQ=0)

0 1 0 1 0 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Defined in IEC 60870-5-101 or IEC 60870-5-104	ENCAPSULATED ASDU Defined in IEC 60870-5-101 or IEC 60870-5-104 Includes Data Unit Identifier and Information Object(s) of that ASDU	
Value	CSQ = Challenge sequence number, defined in 7.2.4.3 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User Number, defined in 7.2.4.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in HLN	MAC value, defined in 7.2.4.5 of IEC/TS 62351-5:2013	

Figure 6 – ASDU: S_AR_NA_1 Aggressive Mode Authentication Request

S_AR_NA_1:= CP{Data unit identifier, ENCAPSULATED ASDU,CSQ, USR, MAC Value }

CAUSES OF TRANSMISSION used with
TYPE IDENT 83:= S_AR_NA_1

CAUSE OF TRANSMISSION

In control direction:

<14>:= authentication

In monitor direction:

<14>:= authentication

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

7.3.4 TYPE IDENT 84: S_KR_NA_1 Session key status request

The structure of this ASDU is defined in Figure 7.

Single information object (SQ=0)

0 1 0 1 0 1 0 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
Value	USR = User Number, defined in 7.2.4.4 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		

Figure 7 – ASDU: S_KR_NA_1 Session key status request

S_KR_NA_1:= CP{Data unit identifier, USR }

CAUSES OF TRANSMISSION used with
TYPE IDENT 84:= S_KR_NA_1

CAUSE OF TRANSMISSION

In control direction:

<15>:= maintenance of authentication session key

In monitor direction:

<44>:= unknown type identification

7.3.5 TYPE IDENT 85: S_KS_NA_1 Session key status

The structure of this ASDU is defined in Figure 8.

Single information object (SQ=0)

0 1 0 1 0 1 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Value Value Value Value	KSQ = Key change sequence number, defined in 7.2.6.2 of IEC/TS 62351-5:2013	
Value Value	USR = User Number, defined in 7.2.6.3 of IEC/TS 62351-5:2013	
Enumerated value	KWA = Key wrap algorithm, defined in 7.2.6.4 of IEC/TS 62351-5:2013	
Enumerated value	KST = Key status, defined in 7.2.6.5 of of IEC/TS 62351-5:2013	
Enumerated value	HAL = MAC algorithm, defined in 7.2.6.6 of of IEC/TS 62351-5:2013	
Value Value	CLN = Challenge data length, defined in 7.2.6.7 of of IEC/TS 62351-5:2013. Zero if KST does not equal <0> OK.	
Number of octets specified in CLN	Pseudo-random challenge data, defined in 7.2.6.8 of of IEC/TS 62351-5:2013	
Number of octets specified in HAL	MAC value, defined in 7.2.6.9 of of IEC/TS 62351-5:2013. Only included if KST = <0> OK.	

Figure 8 – ASDU: S_KS_NA_1 Session key status

S_KS_NA_1:= CP{Data unit identifier, KSQ, USR, KWA, KST, HAL, CLN, Pseudo-random challenge data, MAC value }

CAUSES OF TRANSMISSION used with
TYPE IDENT 85:= S_KS_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<15>:= maintenance of authentication session key

7.3.6 TYPE IDENT 86: S_KC_NA_1 Session key change

The structure of this ASDU is defined in Figure 9.

Single information object (SQ=0)

0 1 0 1 0 1 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Value	KSQ = Key Change sequence number, defined in 7.2.7.2 of IEC/TS 62351-5:2013	
Value		
Value		
Value		
Value	USR = User Number, defined in 7.2.7.3 of IEC/TS 62351-5:2013	
Value		
Value	WKL = Wrapped key data length, defined in 7.2.7.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in WKL	Wrapped key data, defined in 7.2.7.5 of IEC/TS 62351-5:2013	

Figure 9 – ASDU: S_KC_NA_1 Session key change

S_KC_NA_1:= CP{Data unit identifier, KSQ, USR, WKL, Key Data }

CAUSES OF TRANSMISSION used with
TYPE IDENT 86:= S_KC_NA_1

CAUSE OF TRANSMISSION

In control direction:

<15>:= maintenance of authentication session key

In monitor direction:

<44>:= unknown type identification

7.3.7 TYPE IDENT 87: S_ER_NA_1 Authentication error

The structure of this ASDU is defined in Figure 10.

Single information object (SQ=0)

0 1 0 1 0 1 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Value Value Value Value	CSQ = Challenge Sequence number, defined in 7.2.2.2 of IEC/TS 62351-5:2013 or, KSQ = Key change sequence number, defined in 7.2.6.2 of IEC/TS 62351-5:2013	
Value Value	USR = User Number, defined in 7.2.8.3 of IEC/TS 62351-5:2013	
Value Value	AID = Association ID, defined in 7.2.8.4 of IEC/TS 62351-5:2013	
Enumerated value	ERR = Error code, defined in 7.2.8.5 of IEC/TS 62351-5:2013	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	ETM = Error time stamp, 7-octet binary time	
Value Value	ELN = Error length, defined in 7.2.8.6 of IEC/TS 62351-5:2013	
Number of octets specified in ELN	Error text, defined in 7.2.8.7 of IEC/TS 62351-5:2013	

Figure 10 – ASDU: S_ER_NA_1 Authentication error

S_ER_NA_1:= CP{Data unit identifier, CSQ/KSQ, USR, AID, ERR, ETM, ELN, Error Text }

CAUSES OF TRANSMISSION used with
TYPE IDENT 87:= S_ER_NA_1

CAUSE OF TRANSMISSION

In control direction:

<14>:= authentication

In monitor direction:

<14>:= authentication

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

7.3.8 TYPE IDENT 88: S_UC_NA_1 User certificate

This ASDU Type may be used in place of S_US_NA_1 User Status Change for making changes to Update Keys using asymmetric Key Change Methods.

The structure of this ASDU is defined in Figure 11.

Single information object (SQ=0)

0 1 0 1 0 1 0 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Enumerated value	KCM = Key Change Method, defined in 7.2.9.2 of IEC/TS 62351-5:2013	
Value	CDL = Certification Data Length, defined in 7.2.9.9 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in CDL	Certification Data. A standard X.509 certificate as described in RFC 5280 and refined for role-based access control of power system data communications as described in IEC/TS 62351-8.	

Figure 11 – ASDU: S_UC_NA_1 User certificate

S_UC_NA_1:= CP{Data unit identifier, KCM, CDL, Certification Data }

CAUSES OF TRANSMISSION used with
TYPE IDENT 90:= S_UC_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of user role and update key

In monitor direction:

<44>:= unknown type identification

7.3.9 TYPE IDENT 90: S_US_NA_1
User status change

The structure of this ASDU is defined in Figure 12.

Single information object (SQ=0)

0 1 0 1 1 0 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Enumerated value	KCM = Key Change Method, defined in 7.2.9.2 of IEC/TS 62351-5:2013	
Enumerated value	OPR = Operation, defined in 7.2.9.3 of IEC/TS 62351-5:2013	
Value	SCS = Status Change Sequence number, defined in 7.2.9.4 of IEC/TS 62351-5:2013	
Value		
Value		
Value		
Value	URL = User Role, defined in 7.2.9.5 of IEC/TS 62351-5:2013	
Value		
Value	UEI = User Role Expiry Interval, defined in 7.2.9.6 of IEC/TS 62351-5:2013	
Value		
Value	UNL = User Name Length, defined in 7.2.9.7 of IEC/TS 62351-5:2013	
Value		
Value	UKL = User Public Key Length, defined in 7.2.9.8 of IEC/TS 62351-5:2013	
Value		
Value	CDL = Certification Data Length, defined in 7.2.9.9 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in UNL	User Name, defined in 7.2.9.10 of IEC/TS 62351-5:2013	
Number of octets specified in UKL	User public key, defined in 7.2.9.11 of IEC/TS 62351-5:2013	
Number of octets specified in CDL	Certification data, defined in 7.2.9.12 of IEC/TS 62351-5:2013	

Figure 12 – ASDU: S_US_NA_1 User status change

S_US_NA_1:= CP{Data unit identifier, KCM, OPR, SCS, URL, UEI, UNL, UKL, CDL, User name, User public key, Certification data }

CAUSES OF TRANSMISSION used with
TYPE IDENT 90:= S_US_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of user role and update key

In monitor direction:

<44>:= unknown type identification

7.3.10 TYPE IDENT 91: S_UQ_NA_1 Update key change request

The structure of this ASDU is defined in Figure 13.

Single information object (SQ=0)

0 1 0 1 1 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Enumerated value	KCM = Key change method, defined in 7.2.9.2 of IEC/TS 62351-5:2013	
Value	UNL = User name length, defined in 7.2.10.3 of IEC/TS 62351-5:2013	
Value		
Value	CCL = Controlling station challenge data length, defined in 7.2.10.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in UNL	User name, defined in 7.2.10.5 of IEC/TS 62351-5:2013	
Number of octets specified in CCL	Controlling station challenge data, defined in 7.2.10.6 of IEC/TS 62351-5:2013	

Figure 13 – ASDU: S_UQ_NA_1 Update key change request

S_UQ_NA_1:= CP{Data unit identifier, KCM, UNL, CCL, User name, Controlling station challenge data}

CAUSES OF TRANSMISSION used with
TYPE IDENT 91:= S_UQ_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of user role and update key

In monitor direction:

<44>:= unknown type identification

7.3.11 TYPE IDENT 92: S_UR_NA_1
Update key change reply

The structure of this ASDU is defined in Figure 14.

Single information object (SQ=0)

0 1 0 1 1 1 0 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Value	KSQ = Key Change Sequence number, defined in 7.2.11.2 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User number, defined in 7.2.11.3 of IEC/TS 62351-5:2013	
Value		
Value	CDL = Challenge data length, defined in 7.2.11.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in CDL	Controlled station challenge data, defined in 7.2.11.5 of IEC/TS 62351-5:2013	

Figure 14 – ASDU: S_UR_NA_1 Update key change reply

S_UR_NA_1:= CP{Data unit identifier, KSQ, USR, CDL, Controlled station challenge data }

CAUSES OF TRANSMISSION used with
TYPE IDENT 92:= S_UR_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<16>:= maintenance of user role and update key

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

7.3.12 TYPE IDENT 93: S_UK_NA_1
Update key change – symmetric

The structure of this ASDU is defined in Figure 15.

Single information object (SQ=0)

0 1 0 1 1 1 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Value	KSQ = Key Change Sequence number, defined in 7.2.12.2 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User number, defined in 7.2.12.3 of IEC/TS 62351-5:2013	
Value		
Value	EUL = Encrypted update key length, defined in 7.2.12.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in EUL	Encrypted update key, defined in 7.2.12.5 of IEC/TS 62351-5:2013	
Number of octets specified in Table 27 of IEC/TS 62351-5:2013	Message Authentication Code, described in 7.2.14.2 of IEC/TS 62351-5:2013	

Figure 15 – ASDU: S_UK_NA_1 Update key change – symmetric

S_UK_NA_1:= CP{Data unit identifier, KSQ, USR, EUL, Encrypted update key, Message Authentication Code }

CAUSES OF TRANSMISSION used with
TYPE IDENT 93:= S_UK_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of user role and update key

In monitor direction:

<44>:= unknown type identification

NOTE The ASDU S_UK_NA_1 is the concatenation of the Update Key Change message and Update Key Change Confirmation message from IEC/TS 62351-5.

7.3.13 TYPE IDENT 94: S_UA_NA_1
Update key change – asymmetric

The structure of this ASDU is defined in Figure 16.

Single information object (SQ=0)

0 1 0 1 1 1 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	
Value	KSQ = Key Change Sequence number, defined in 7.2.12.2 of IEC/TS 62351-5:2013	INFORMATION OBJECT
Value		
Value		
Value		
Value	USR = User number, defined in 7.2.12.3 of IEC/TS 62351-5:2013	
Value		
Value	EUL = Encrypted update key length, defined in 7.2.12.4 of IEC/TS 62351-5:2013	
Value		
Number of octets specified in EUL	Encrypted update key, defined in 7.2.12.5 of IEC/TS 62351-5:2013	
Number of octets specified in Table 25 of IEC/TS 62351-5:2013	Digital signature, described in 7.2.13.2 of IEC/TS 62351-5:2013	

Figure 16 – ASDU: S_UA_NA_1 Update key change – asymmetric

S_UA_NA_1:= CP{Data unit identifier, KSQ, USR, EUL, Encrypted update key, Digital signature }

CAUSES OF TRANSMISSION used with
TYPE IDENT 94:= S_UA_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of user role and update key

In monitor direction:

<44>:= unknown type identification

NOTE The ASDU S_UA_NA_1 is the concatenation of the Update Key Change message and Update Key Change Signature message from IEC/TS 62351-5.

7.3.14 TYPE IDENT 95: S_UC_NA_1
Update key change confirmation

The structure of this ASDU is defined in Figure 17.

Single information object (SQ=0)

0 1 0 1 1 1 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 7.2.5	INFORMATION OBJECT
Number of octets specified in Table 27 of IEC/TS 62351-5:2013	Message Authentication Code, described in 7.2.14.2 of IEC/TS 62351-5:2013	

Figure 17 – ASDU: S_UC_NA_1 Update key change confirmation

S_UC_NA_1:= CP{Data unit identifier, Message Authentication Code }

CAUSES OF TRANSMISSION used with
TYPE IDENT 95:= S_UC_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<16>:= maintenance of user role and update key

7.3.15 TYPE IDENT 41: S_IT_TC_1
Integrated totals containing time-tagged security statistics

The structure of this ASDU is defined in Figure 18.

0 0 1 0 1 0 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 Number i of objects	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
Defined in 7.2.5 of IEC 60870-5-101:2003	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT 1
Value	AID = Association ID, defined in 7.2.8.4 of IEC/TS 62351-5:2013	
Value		
Value	BCR = Binary counter reading, defined in 7.2.6.9 of IEC 60870-5-101:2003	
Value		
Value		
S Value		
IV CA CY Sequence number		
CP56Time2a Defined in 7.2.6.18 of IEC 609870-5-101:2003	Seven octet binary time	
Defined in 7.2.5 of IEC 60870-5-101:2003	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT i
Value	AID = Association ID, defined in 7.2.8.4 of IEC/TS 62351-5:2013	
Value		
Value	BCR = Binary counter reading, defined in 7.2.6.9 of IEC 60870-5-101:2003	
Value		
Value		
S Value		
IV CA CY Sequence number		
CP56Time2a Defined in 7.2.6.18 of IEC 609870-5-101:2003	Seven octet binary time	

Figure 18 – ASDU: S_IT_TC_1
Integrated totals containing time-tagged security statistics

S_IT_TC_1:= CP{Data unit identifier, information object address, AID, BCR, CP56Time2a }
i:= number of objects defined in the variable structure qualifier

CAUSES OF TRANSMISSION used with
TYPE IDENT 41:= S_IT_TC_1

CAUSE OF TRANSMISSION

In monitor direction:

<3> := spontaneous

<37>:= requested by general counter request

<38>:= requested by group 1 counter request

<39>:= requested by group 2 counter request

<40>:= requested by group 3 counter request

<41>:= requested by group 4 counter request

<44>:= unknown type identification

<45>:= unknown cause of transmission

<46>:= unknown common address of ASDU

8 Implementation of procedures

8.1 Overview of clause

Stations implementing this specification for security of IEC 60870-5-101/IEC 60870-5-104 shall implement the procedures and state machines described in 7.3 of IEC/TS 62351-5:2013. They shall also implement the additional procedures described in the remainder of this clause.

8.2 Initialization of aggressive mode

Aggressive mode shall be the normal method of authentication for stations implementing this specification. To initialize the challenge data in each direction so that aggressive mode can be used, the following procedures shall be followed, as illustrated in Figure 19:

1) The End of Initialization ASDU (M_EI_NA_1) which is listed as optional in IEC 60870-5-101 and IEC 60870-5-104, is recommended for implementation with IEC 60870-5-7.
2) The controlled station shall not send any further data ASDUs until the controlling station has been authenticated.
3) Upon receiving the End of Initialization (M_EI_NA_1) from the controlled station or otherwise detecting that communications has been re-established (e.g. a STARTDT confirmation), the controlling station shall initialize the Session Keys, beginning with the transmission of a Session Key Status Request (S_KR_NA_1). The controlled and controlling stations shall complete the Session Key initialization process as described in IEC/TS 62351-5.
4) The Test Command ASDU (C_TS_NA_1), which is listed as optional in IEC 60870-5-101 and IEC 60870-5-104, shall be mandatory for compliance with IEC 60870-5-7.
5) After the controlling station finishes the process of periodically changing Session Keys as described in IEC/TS 62351-5, the controlling station shall issue a Test Command activation (C_TS_NA_1 act) to the controlled station.
6) The controlled station shall transmit an Authentication Challenge (S_CH_NA_1) to the Test Command activation (C_TS_NA_1 act).
7) The controlling station shall respond with a correctly-formed Authentication Reply (S_RP_NA_1).
8) When the Test Command activation (C_TS_NA_1 act) from the controlling station has been successfully authenticated, the controlled station shall respond with the appropriate confirmation (C_TS_NA_1 con) ASDU.
9) The controlling station shall transmit an Authentication Challenge (S_CH_NA_1) to the Test Command confirmation (C_TS_NA_1 con).

10) The controlled station shall respond with a correctly-formed Authentication Reply (S_RP_NA_1).

11) All critical functions following the exchange of challenges to the Test Command activation and confirmation shall be authenticated using aggressive mode, for instance time synchronization (C_CS_NA_1) and general interrogation (C_IC_NA_1), if the two stations consider them to be critical. If a station attempts to perform a critical function in non-aggressive mode, i.e. sending it as an unauthenticated ASDU, the receiving station shall not challenge the ASDU as described in IEC/TS 62351-5. Instead, the receiving station shall increment the Unexpected Messages statistic but otherwise behave as if the ASDU had not been transmitted.

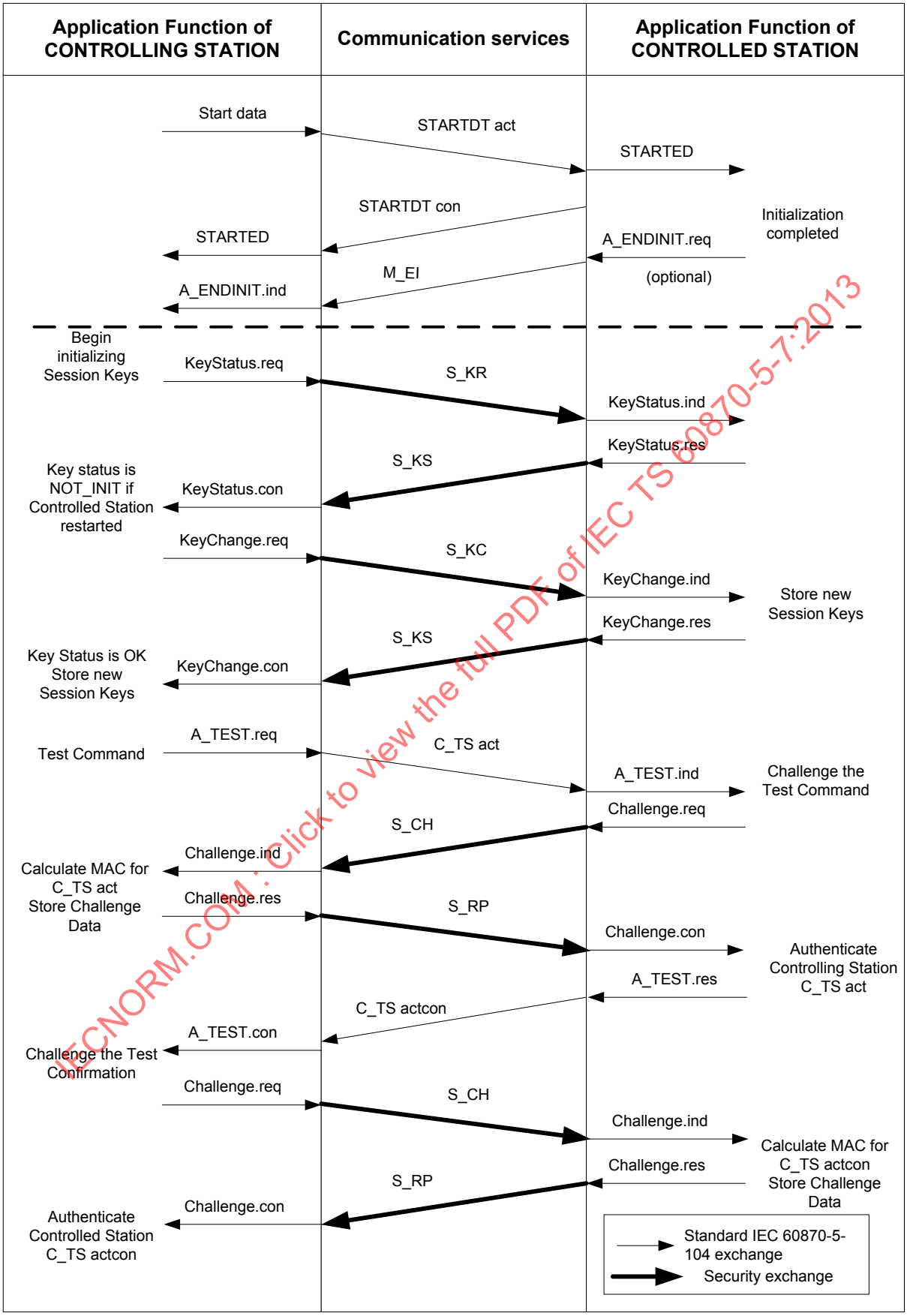


Figure 19 – Example of successful initialization of challenge data

8.3 Refreshing challenge data

To refresh the challenge data in each direction so that aggressive mode can be used, the controlling station shall repeat the steps illustrated below the dashed line in Figure 19 whenever it is time to periodically refresh the Session Keys, including the challenge / response sequence with the C_TS (Test Command). All critical functions following the exchange of challenges to the Test Command activation and confirmation shall be authenticated using aggressive mode,

If the challenge / response authentication process for the Test Command fails for any reason, the stations shall follow the recovery procedures described in IEC/TS 62351-5. The controlling station may retry the Test Command sequence until the Max Authentication Failures limit is exceeded. In accordance with IEC/TS 62351-5, neither station shall perform critical functions until the challenge data has been refreshed.

8.4 Co-existence with non-secure implementations

It shall be configurable at the controlling station whether to apply this specification on a per-connection and per data link address basis. This will permit secure and non-secure controlled station implementations to communicate with the same controlling station at the same time.

9 Implementation of IEC/TS 62351-3 using IEC 60870-5-104

9.1 Overview of clause

IEC 60870-5-104 implementations claiming compliance to this specification shall implement Transport Layer Security (TLS) according to IEC/TS 62351-3 in addition to application layer authentication per IEC/TS 62351-5. IEC 60870-5-104 implementations shall comply with the following requirements taken from IEC/TS 62351-3:2007. *Italicized text* is a direct quotation from IEC/TS 62351-3:2007.

9.2 Deprecation of non-encrypting cipher suites

Any cipher suite that specifies NULL for encryption shall not be used. The list of deprecated suites includes, but is not limited to:

TLS_NULL_WITH_NULL_NULL

TLS_RSA_NULL_WITH_NULL_MD5

TLS_RSA_NULL_WITH_NULL_SHA

9.3 Mandatory cipher suite

IEC 60870-5-104 implementations that use TLS shall support the following cipher suite at a minimum:

TLS_RSA_WITH_AES_128_SHA

This is the mandatory cipher suite for TLS version 1.2.

9.4 Recommended cipher suites

It is recommended that IEC 60870-5-104 implementations using TLS support the following cipher suites. Implementations may also choose to implement cipher suites not listed here.

Table 5 – Recommended cipher suite combinations

Key exchange		Encryption	Hash
Algorithm	Signature		
TLS_DH_	DSS_	WITH_AES_128_	SHA
TLS_DH_	DSS_	WITH_AES_256_	SHA
TLS_DH_		WITH_AES_128_	SHA
TLS_DH_		WITH_AES_256_	SHA

9.5 Negotiation of versions

Only TLS 1.0 corresponding to SSL version 3.1 (or higher) shall be allowable. Proposal of version prior to SSL 3.1 shall result in no connection being established.

9.6 Cipher renegotiation

Implementations claiming conformance to this standard shall specify that the symmetric keys shall be renegotiated based upon a time period and a maximum allowed number of packets/bytes sent. It is a PIXIT issue, of the referencing standard, to specify the constraints on the renegotiation.

The renegotiation values shall be configurable.

IEC 60870-5-104 implementations using TLS shall renegotiate the TLS symmetric keys when the application layer Session Key Change Interval expires or the Session Key Change Count is exceeded. It is recommended that TLS renegotiation take place before the application layer key change.

The initiation of the change cipher sequence shall be the responsibility of the TCP entity that receives the TCP-OPEN indication (e.g. the called entity). A request to change the cipher, issued from the calling entity (e.g. the node that issued the TCP-OPEN) shall be ignored.

There shall be a timeout associated with the response to a change cipher request. A timeout of the change cipher request shall result in the connection being terminated. The timeout value shall be configurable.

IEC 60870-5-104 implementations using TLS shall use a change cipher request timeout configurable in the same range as the application security reply timeout described in IEC/TS 62351-5.

9.7 Message authentication code

The Message Authentication Code shall be used.

NOTE TLS has this capability specified as an option. This standard mandates the use of this capability to aid in countering and detection of man-in-the-middle attacks.

9.8 Certificate support

9.8.1 Overview of clause

IEC 60870-5-104 Implementations using Transport Layer Security (TLS) shall comply with the following requirements for certificate management taken from IEC/TS 62351-3.

When operating over TCP/IP, it may be possible to change and distribute Update Keys by making use of other IP-based security protocols. However, such mechanisms are outside the scope of this specification.

9.8.2 Multiple Certificate Authorities (CAs)

An implementation, claiming conformance to this standard, shall support more than one Certificate Authority.

IEC 60870-5-104 Implementations using TLS shall support at least four Certificate authorities.

The actual number shall be declared in the implementation's Device Profile Document.

The criteria and selection of a CA is out-of-scope of this standard.

9.8.3 Certificate size

A protocol, specifying the use of this standard, shall specify the maximum size of certificate allowed to be used. It is recommended that this size shall be less than or equal to 8 192 bytes.

IEC 60870-5-104 implementations using TLS shall support a minimum-maximum certificate size of 8 192 octets. It is a local issue if larger certificates are supported.

An implementation that receives a certificate larger than the size that it can support shall terminate the connection.

9.8.4 Certificate exchange

The certificate exchange, and validation, shall be bi-directional. If either entity does not provide its certificate, the connection shall be terminated.

9.8.5 Certificate comparison

9.8.5.1 General

Certificates shall be validated by both the calling and called nodes. There are two mechanisms that shall be configurable for certificate verification.

- *Acceptance of any certificate from an authorized CA*
- *Acceptance of individual certificates from an authorized CA*

9.8.5.2 Verification based upon CA

An implementation, claiming conformance to this standard, shall be capable of being configured to accept certificates from one or more Certificate Authorities without the configuration of individual certificates.

9.8.5.3 Verification based upon individual certificates

An implementation, claiming conformance to this standard, shall be capable of being configured to accept specific individual certificates from one or more authorized Certificate Authorities (e.g. configured).

9.8.5.4 Certificate revocation

Certificate revocation shall be performed as specified in RFC 3280.

NOTE Since IEC/TS 62351-3:2007 was published, RFC 3280 has been obsoleted by RFC 5280.

The management of the Certificate Revocation List (CRL) is a local implementation issue.