IEC TS 62351-100-1

Edition 1.0 2018-11

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7

IEC TS 62351-100-1:2018-11(en)

IEC Central Office
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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 TS 62351-100-1

Edition 1.0 2018-11

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communications security – Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-6182-8

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7

FOREWORD

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

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

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

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

IEC TS 62351-100-1, 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
57/1980/DTS	57/2016/RVDTS

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

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://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.

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.

INTRODUCTION

This technical specification describes test cases for conformance testing of telecontrol equipment or systems using the IEC TS 62351-5 security extension and its application in IEC TS 60870-5-7 for IEC 60870-5-101 and IEC 60870-5-104 communication protocols.

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

Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7

1 Scope

This part of IEC 62351, which is a technical specification, describes test cases of data and communication security for telecontrol equipment, substation automation systems (SAS) and telecontrol systems, including front-end functions of SCADA.

The goal of this document is to enable interoperability by providing a standard method of testing protocol implementations to verify that a device fulfils the requirement of the standard. Note that conformity to the standard does not guarantee interoperability between devices using different implementations. It is expected that using this specification during testing will minimize the risk of non-interoperability. A basic condition for this interoperability is a passed conformance test of both devices.

The scope of this document is to specify commonly available procedures and definitions for conformance and/or interoperability testing of IEC TS 62351-5 and IEC TS 60870-5-7. The conformance test cases defined herein are focused to verify the conformant integration of the underlying authentication, as specified in IEC TS 62351-5 and IEC TS 60870-5-7, to protect IEC 60870-5-101 and IEC 6870-5-104-based communications.

This document deals with data and communication security conformance testing; therefore, other requirements, such as safety or EMC, are not covered. These requirements are covered by other standards (if applicable) and the proof of compliance for these topics is done according to these standards.

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.[1]

IEC 60870-5-6:2006, *Telecontrol equipment and systems – Part 5-6: Guidelines for conformance testing for the IEC 60870-5 companion standards*l

IEC TS 60870-5-7:2013, *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 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

1 The base standard always takes precedence. In case of ambiguity between this document and the base standards (IEC TS 62351-5 and IEC TS 60870-5-7), this part of IEC 62351 needs to be clarified or amended.

When testing, negative behaviour is not described in the base standard. The behaviour described in this document prevails and should be observed. The conformance statement produced after testing indicates any lack of conformance to either the test plan or the base standard.

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 60870-5-601:2015, *Telecontrol equipment and systems – Part 5-601: Transmission protocols – Conformance test cases for the IEC 60870-5-101 companion standard*

IEC TS 60870-5-604:2016, *Telecontrol equipment and systems – Part 5-604: Conformance test cases for the IEC 60870-5-104 companion standard*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

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 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

3 Terms, definitions and abbreviated terms

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 Terms and definitions

3.1.1
Application Service Data Unit
ASDU
application layer message submitted to lower layers for transmission

3.1.2
control direction
direction of transmission from the controlling station to a controlled station

3.1.3
controlled station
station which is monitored, or commanded and monitored by a master (controlling) station

Note 1 to entry: This is commonly called an “outstation” or “slave” or “server” in some specifications.

3.1.4
controlling station
station which performs the telecontrol of outstations (controlled station)

Note 1 to entry: This is commonly called a “master” or “master station” or “client” in some specifications.

3.1.5
interoperability
ability of two or more telecontrol devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation

3.1.6
Message Authentication Code
MAC
calculated value used by a receiving station to authenticate and check the integrity of an information

3.1.7
monitor direction
direction of transmission from a controlled station to a controlling station

3.1.8
normal procedure tests
set of test cases to verify that the device fulfils the requirements of the standard in the expected (normal) conditions

3.1.9
Protocol Implementation Conformance Statement
PICS
summary of the referencing standard capabilities of the system to be tested

3.1.10
Protocol Implementation Document
PID
document which describes complete functionalities and system specific information

Note 1 to entry: The PID consists of the PICS and the PIXIT.

3.1.11
Protocol Implementation eXtra Information for Testing
PIXIT
document containing system specific information regarding the capabilities of the system to be tested and specifying which items are optional

3.1.12
resiliency tests
set of test cases to verify that the device fulfils the requirements of the standard in reacting to the unexpected (error) conditions

3.1.13
test equipment
all tools and instruments which simulate and verify the communication traffic, input or outputs of the system under test

3.1.14
test initiator
party initiating a conformance test of a device that is executed by a test facility

3.1.15
test facility
supplier-independent organization which is able to provide appropriate test equipment and trained staff for conformance testing

3.1.16
user number
USR
numeric value that unambiguously identifying a user in the protocol

3.2 Abbreviated terms

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

ASDU	Application service data unit
CASDU	Common address of ASDU
COT	Cause of transmission
DUT	Device under test
IOA	Information object address
IP	Inter-networking protocol
MAC	Message authentication code
PICS	Protocol implementation conformance statement
PID	Protocol implementation document (=PICS + PIXIT)
PIXIT	Protocol implementation extra information for testing
SAS	Substation automation system
SCADA	Supervisory control and data acquisition
TCP	Transport control protocol
USR	User number

4 General

4.1 Normatives covered by this technical specification

This document defines the conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 and the security extensions for IEC 60870-5-101 and IEC 60870-5-104 base protocols.

Test cases for IEC 60870-5-101 and IEC 60870-5-104 base protocols are not in the scope of this document since they are already defined respectively in IEC TS 60870-5-601 and IEC TS 60870-5-604.

4.2 Conformance testing structure

4.2.1 General

The security extension defined in IEC TS 62351-5 and IEC TS 60870-5-7 introduces new procedures and new ASDU types to be exchanged at application level, each procedure has its own set of messages exchanged during execution.

The conformance test cases are divided into five clauses:

- Clause 5: Verification of configuration parameters. This clause contains the configuration parameters affecting the message contents and/or the protocol behaviour.
- Clause 6: Verification of communication. The goal of this clause is to verify that DUT is able to implement the security extension messages as described in IEC TS 60870-5-7.
- Clause 7: Verification of procedures. The goal of this clause is to verify that DUT is able to execute the security extension procedures as described in IEC TS 62351-5.
- Clause 8: Test result chart. This clause contains the results of the test cases listed in Clauses 6 and 7 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables (see Tables 4 to 56). They are numbered; their numbering syntax is: Subclause number (where the Table is located) + test case number.

In the column ‘reference’ each test case has a direct reference to IEC TS 62351-5 or IEC TS 60870-5-7 where the clause under test is defined.

Test cases are mandatory depending on the description in the column ‘Required’. The following situations are possible:

M = Mandatory test case. The test is referencing a clause that is mandatory in IEC TS 62351-5 or IEC TS 60870-5-7.

PICS x, x = Mandatory test case if the functionality is enabled in the PICS (by marking the applicable check box), with a reference to the section number of the PICS (x.x).

4.2.2 Conformance testing of security extension procedures

The security extension procedures can be summarized as follows:

- User management
- Update key maintenance
- Session key maintenance
- Challenge/Reply authentication
- Aggressive Mode authentication

In general, these procedures are executed in sequence as shown in Figure 1.

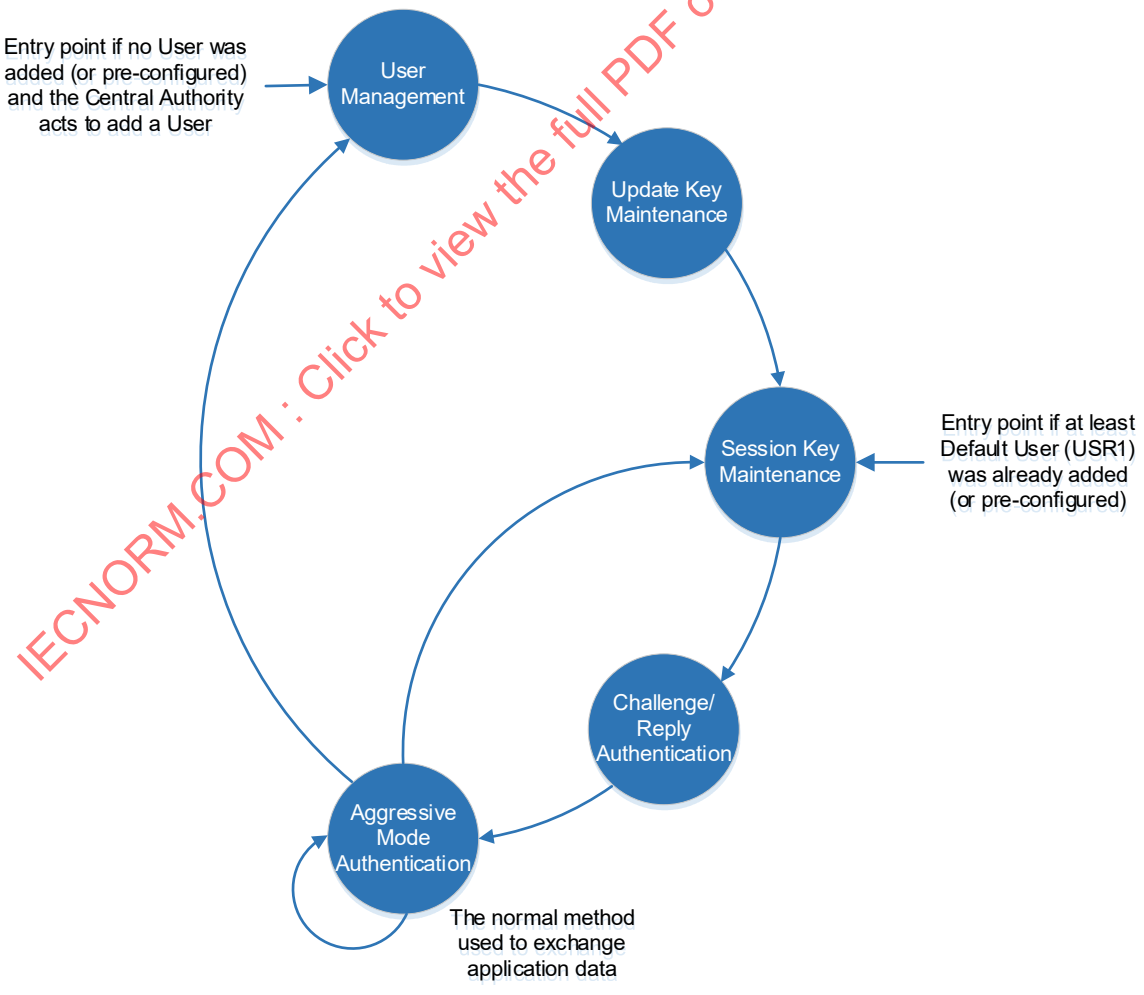

Figure 1 – IEC TS 62351-5 Security extension procedures

This document follows this approach. Conformance tests listed in Clauses 6 and 7 are organized into subclauses for each security extension procedure.

4.2.3 Conformance testing addressed per station type

The security extension procedures defined in IEC TS 62351-5 and the messages exchanged in each of them defined in IEC TS 60870-5-7 are almost asymmetric per station type (controlling or controlled). The test cases in Clause 7 are addressed per station type.

4.2.4 Normal procedure tests and resiliency tests

The IEC TS 62351-5 state machine specifies how each station (controlling and controlled) shall execute the procedures in normal conditions (expected behavior) and also how it shall behave when unexpected or fault events occur during their execution (negative behaviours). So, for each procedure in Clause 7 the tests cases are also divided in two sections: the normal procedures test cases addressing the expected behaviours and the resiliency test cases addressing unexpected or fault events.

Normal Procedure tests and resiliency tests shall be performed for ALL mandatory and optional security extension procedures implemented (declared in the PICS document).

Normal Procedure tests shall be performed AT LEAST ONCE for all mandatory and optional authentication and key encryption algorithms implemented (declared in the PICS document).

The resiliency test shall be performed AT LEAST ONCE with an authentication algorithm and an encryption algorithm defined as mandatory in IEC TS 62351-5.

4.3 Conformance testing requirements

4.3.1 Testing base protocols with security extension

The implementations claiming conformance to the IEC TS 62351-5 shall permit the authentication (the security extension) to be disabled (see IEC TS 62351-5:2013, 8.2.5.8). When the security extension is disabled the communication is achieved through the IEC 60870-5-101 or IEC 60870-5-104 base protocol so the conformance tests shall also be executed on the base protocol following its own conformance testing standard (IEC 60870-5-601 or IEC TS 60870-5-604).

The conformance testing of the base protocol shall be performed prior to execution of the security extension conformance testing. The test initiator shall provide the evidence that the base protocol conformance testing was successfully performed for the DUT. Once the base protocol conformance test is successfully completed, the security extension shall be enabled and tested as defined in this technical specification.

While testing the security extension, some test cases require the use of base protocol ASDU to be sent/received and authenticated. The test facility shall verify that the base protocol data exchanged and the base protocol procedures executed by the DUT also are in accordance with the type of base protocol ASDU used for authentication, as specified in IEC 60870-5-101 or IEC 60870-5-104. This verification shall be performed by following the base protocol conformance testing standard (IEC 60870-5-601 or IEC TS 60870-5-604).

4.3.2 Testing of profiles including TCP/IP

For profiles including TCP/IP (i.e. IEC 60870-5-104) the conformance testing of IEC 62351-3 (defined in IEC 62351-100-3) is also required.

4.3.3 Requirements for the device under test

The entity submitting the device for testing shall provide the following:

a) The device ready for testing;

b) The Protocol Implementation Document (PID);

c) Instruction manuals detailing the installation and operation of the device or assistance for operating the DUT during the test.

A device is ready for testing when the following conditions are satisfied:

d) The DUT is able to operate as a controlling or controlled station according to the PID (depending of the type of DUT).

e) The DUT shall be fully configured according to the PID, and shall be able to execute all the functionality of the protocol implementation as described in the PID.

f) The functionality described in the PID related to data points such as parameter loading, read procedure, command transmission, etc. is implemented with a representative sub-set of data points.

g) Verification of the data points shall be possible in a human readable way or format, and the verification of analogue and digital status changes is possible.

4.3.4 Requirements for the test facility

The following requirements shall be satisfied by the test facility:

- Conformance testing shall be customized for the DUT based on the capabilities identified in the PID (=PICS+PIXIT). Upon this customization, the test facility shall communicate what the tailored test plan will cover.
- The test cases listed in Clauses 5 to 7 shall be performed with no errors detected during testing.
- The test cases listed in Clause 6 (verification of communication) are automatically tested while executing the test cases listed in Clause 7 (verification of procedures).
- The test cases in Clause 7 should be performed in the order listed and the steps in each test case shall be followed, which means that the DUT is able to function as described in the specific test case.
- For each test case listed in Clauses 5, 6 and 7 the test results need to be marked in the appropriate column of the test result chart in Clause 8. Each test case can either pass the test (Passed), fail the test (Failed), not applicable, when the configuration value is not supported by the device (N.A.), or the test case was not performed (Empty). Ideally, there should be no empty boxes when testing is complete.
- Release a conformance test report of the DUT to the initiator (refer to IEC 60870-5-6:2006, 5.7).

All test cases listed in Clauses 6 and 7 should be verified automatically by a testing software or verified manually by review of the test history log after execution of the test procedures. The simulator is preferably flexible in adding or changing test cases in order to be adaptable to changes in the protocol standard and the PID provided with the DUT. In all cases, the test shall be reproducible over time by test-engineers in the test-facility.

In operational use, the device may show communication and/or behaviour errors which forces the supplier to reproduce the complete conformance test (for example for verification afterwards) or for reproducing only the tests that were shown to have errors.

The test focuses only on the protocol elements and functions as described in the PID; the test does not include the application logic and the operation of the tested system.

4.3.5 Test logging

During the execution of conformance testing the following information shall be logged by the DUT for test results analysis:

- Communication events (messages received/sent and their fields content).

Furthermore, the DUT should be able to log the following:

- Internal events (timeouts, statistic threshold exceeded).
- Internal actions (key status changes, statistic counters changes, messages discarded, timers start/stop).

5 Verification of configuration parameters

5.1 General

The scope of this clause is to verify the configuration of all the parameters that affect security extension procedures and protocol behaviour so that the whole or part of conformance testing shall be executed (and the tests result chart in Clause 8 shall be filled accordingly) for each value of these parameters as indicated in subclauses below. Basically, the DUT shall be tested to verify that the whole functionality and behaviour are correct according to the configuration(s) defined in the tables below.

5.2 System definition

System definition parameters are defined in the base protocol standard (IEC 60870-5-101 or IEC 60870-5-104). Since these parameters also affect the security extension protocol behaviour, the conformance test procedures listed in Clause 7 and the related ASDU verifications listed in Clause 6 shall be performed as indicated in Table 1.

Table 1 – Configuration parameters: System definition

No.	Test	Definition	Reference	Required
5.2.1	Station Type	Controlling Station (Master), Controlled Station (Outstation)	IEC 60870-5-101:2003, 8.1 IEC 60870-5-104:2006, 9.1	M
		All conformance tests listed in Clauses 6 and 7 shall be performed at least once for each value of this parameter.		
5.2.2	Frame Length	Maximum length L (control direction)	IEC 60870-5-101:2003, 6.2	M
5.2.3		Maximum length L (monitor direction)	IEC 60870-5-101:2003, 8.4 IEC 60870-5-104:2006, 9.5	
		All conformance tests listed in Clauses 6 and 7 shall be performed at least once for each value of these parameters.		
5.2.4	Cause Of Transmission (COT)	Number of octets for Cause of Transmission of ASDU	IEC 60870-5-101:2003, 7.2.3 IEC 60870-5-101:2003, 8.5 IEC 60870-5-104:2006, 9.5	M
		If more than one Cause of Transmission length is supported: a) Perform all Normal Procedure tests and Resiliency tests listed in Clause 7, verifying the communication test listed in Clause 6, for one Cause of Transmission length. b) For the other Cause of Transmission length, perform all Normal Procedure tests listed in Clause 7 verifying the communication test listed in Clause 6.		
5.2.5	Common Address of ASDU (CASDU)	Number of octets for Common Address of ASDU	IEC 60870-5-101:2003, 7.2.4 IEC 60870-5-101:2003, 8.5 IEC 60870-5-104:2006, 9.5	M

No.	Test	Definition	Reference	Required
		If more than one Common Address of ASDU length is supported: a) Perform all Normal Procedure tests and Resiliency tests listed in Clause 7, verifying the communication test listed in Clause 6, for one Common Address of ASDU length. b) For the other Common Address of ASDU length, perform all Normal Procedure tests listed in Clause 7 verifying the communication test listed in Clause 6.		
5.2.6	Information Object Address (IOA)	Number of octets for Information Object Address	IEC 60870-5-101:2003, 7.2.5 IEC 60870-5-101:2003, 8.5 IEC 60870-5-104:2006, 9.5	M
		If more than one Information Object Address length is supported: a) Perform all Normal Procedure tests and Resiliency tests listed in Subclauses 7.5, 7.6 and 7.7 verifying the communication test listed in Clause 6, for one Information Object Address length. b) For the other Information Object Address lengths, perform all Normal Procedure tests listed in Subclauses 7.5, 7.6 and 7.7 verifying the communication test listed in Clause 6		

5.3 Application security extension

Security extension parameters are defined in the IEC TS 62351-5 standard. Since these parameters affect the protocol behaviour, the conformance test procedures listed in Clause 7 and the related ASDU verifications listed in Clause 6 shall be performed for each value of these parameters as indicated in Table 2.

Table 2 – Configuration parameters: Application security extension

No.	Test	Definition	Reference	Required
5.3.1	MAC Algorithm (MAL)	Set of algorithms implemented to calculate MAC of the messages	IEC TS 62351-5:2013, 8.2.2 IEC TS 60870-5-7:2013, 10.3	M
		Normal Procedure tests listed in 7.5, 7.6 and 7.7 shall be performed for each supported (mandatory and optional) MAC Algorithm verifying the communication test listed in Clause 6. Resiliency tests listed in 7.5, 7.6 and 7.7 shall be performed al least once for one mandatory MAC Algorithm verifying the communication test listed in Clause 6.		
5.3.2	Key Wrap Algorithm (KWA)	Set of algorithms implemented to encrypt/decrypt the Session Key	IEC TS 62351-5:2013, 8.2.3 IEC TS 60870-5-7:2013, 10.4	M
		Normal Procedure tests listed in 7.5, 7.6 and 7.7 shall be performed for each supported (mandatory and optional) MAC Algorithm verifying the communication test listed in Clause 6. Resiliency tests listed in 7.5, 7.6 and 7.7 shall be performed at least once for one mandatory MAC Algorithm verifying the communication test listed in Clause 6.		
5.3.3	Update Key Change method (KCM)	Sets of cryptographic algorithms implemented to change the Update Key	IEC TS 62351-5:2013, 8.2.5 IEC TS 60870-5-7:2013,10.6	M
		Normal Procedure tests listed in Clause 7 shall be performed for each supported (mandatory and optional) cryptographic algorithms verifying the communication test listed in Clause 6. Resiliency tests listed in Clause 7 shall be performed at least once for one mandatory cryptographic algorithm verifying the communication test listed in Clause 6.		
5.3.4	User Status Change method	Methods (message) implemented to change the status of a user	IEC TS 62351-5:2013, 7.2.9 IEC TS 60870-5-7:2013, 10.7	M

No.	Test	Definition	Reference	Required
		Normal Procedure tests listed in Clause 7 shall be performed for each supported (mandatory and optional) method verifying the communication test listed in Clause 6. Resiliency tests listed in 8.1, 8.2 and 8.3 shall be performed at least once for one mandatory method verifying the communication test listed in Clause 6.		
5.3.5	Use of Error Messages	Specifies if the Error Messages are used or not.	IEC TS 62351-5:2013, 7.3.3.6 IEC TS 60870-5-7:2013, 10.5	M
		All conformance tests listed in Clause 7 shall be performed at least once for each supported value of this parameter verifying the communication test listed in Clause 6.		
5.3.6	Configurable Parameters	Set of the parameters dynamically involved in secure communication.	IEC TS 62351-5:2013, 8.2.5 IEC TS 60870-5-7:2013, 10.8	M
		All conformance tests listed in Clauses 6 and 7 shall be performed at least once for one combination of these values.		
5.3.7	Configurable statistic thresholds and statistic information object addresses	Set of the statistic counters, their thresholds and their information object addresses used in the Security Statistic message.	IEC TS 62351-5:2013, 7.3.2 IEC TS 62351-5:2013, 8.2.5 IEC TS 60870-5-7:2013, 10.9	M
		All conformance tests listed in Clause 7 shall be performed at least once for one combination of these values.		
5.3.8	Critical functions	List of functions that are considered critical by the DUT.	IEC TS 62351-5:2013, 7.3.3.2 IEC TS 62351-5:2013, 10.3 IEC TS 60870-5-7:2013, 10.10	M
		All conformance tests listed in Clauses 6 and 7 shall be performed at least once for one combination of these values.		

6 Verification of Communication

6.1 General

The purpose of this clause is to verify that the DUT correctly implements the security extension messages, their fields content and their segmentation, as specified in IEC TS 60870-5-7.

6.2 ASDU segmentation control

The Station shall implement the ASDU segmentation control state machine defined in IEC TS 60870-5-7, see Table 3.

Table 3 – ASDU segmentation control

No.	Test	Description	Reference	Required
6.2.1	Transmission of ADSU shorter than or equal to the maximum length of an IEC 60870-5 data link or APCI frame.	Station transmit a single ASDU segment with FIR = 1, FIN = 1, ASN = any sequence number from 0 to 63	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.2	Transmission of ADSU longer than the maximum length of an IEC 60870-5 data link or APCI frame.	Station transmit multiple ASDU segments shorter than or equal to the maximum length of an IEC 60870-5 data link or APCI frame. All segments shall have the same Data Unit Identifiers DUI (TYPE ID, VSQ, COT, CASDU). First segment shall be sent with FIR = 1, FIN = 0, ASN = any sequence number from 0 to 63 Intermediate segments (if there are) shall be sent with FIR = 0, FIN = 0, ASN = last ASN sent + 1 (modulo 64) Last segment shall be sent with FIR = 0, FIN = 1, ASN = last ASN sent + 1 (modulo 64)	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.3	Reception of ASDU segments.	Station shall be able to receive a single ASDU segments shorter than or equal to the maximum length of an IEC 60870-5 data link or APCI frame with both FIR and FIN bits set. Station shall implement the ASDU segments reception and reassembly state machine that acts as specified in IEC TS 60870-5-7.	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.4	Reception of a segment without the FIR bit set while no segment series is in progress	Station shall discard the segment.	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.5	Reception of a segment in which the Type ID, VSQ, CASDU, or COT does not match that of the first ASDU in the segment series in progress.	Station shall discard the segment, the entire in progress segment series and terminate the series.	IEC TS 60870-5-7:2013, 7.2.6	M

No.	Test	Description	Reference	Required
6.2.6	Reception of a segment that is octet-for-octet identical to the preceding segment ASDU in the segment series in progress.	Station shall discard the segment.	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.7	Reception of a segment having the FIR bit set with segment series already in progress.	Station shall discard the entire in progress segment series and start a new segment series with the newly received segment as its first member.	IEC TS 60870-5-7:2013, 7.2.6	M
6.2.8	Reception of a segment having the FIR bit cleared and a sequence number other than the expected incremental number and NOT octet-for-octet identical to the preceding segment	Station shall discard the segment, the entire in progress segment series and terminate the series.	IEC TS 60870-5-7:2013, 7.2.6	M

6.3 Verification of ASDUs

6.3.1 User management ASDUs

Table 4 – User management ASDUs

No.	Test	Description	Reference	Required
6.3.1.1	S_UC_NA_1 ASDU 88 User Certificate	VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.8	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.2	See NOTE (1)	COT: Cause of Transmission Controlling Station values = 16 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.8	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.3		KCM: Key Change Method Value range = <0…255>	IEC TS 62351-5:2013, 7.2.9.2	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.4		CDL: Certification Data Length Value range = <0…65535>	IEC TS 62351-5:2013, 7.2.9.9	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7

No.	Test	Description	Reference	Required
6.3.1.5		CD: Certification Data Sequence of octets of length specified in CDL This field shall contain a valid X.509 certificate provvided by the authority without any modification.	IEC TS 62351-5:2013, 7.2.9.13 IEC TS 60870-5-7:2013, 7.3.8	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.6	S_US_NA_1 ASDU 90 User Status Change	A.1.1.1 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.9	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.7		COT: Cause of Transmission Controlling Station values = 16 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.9	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.8		KCM: Key Change Method Value range = <0...255>	IEC TS 62351-5:2013, 7.2.9.2	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.9		OPR: Operation Value range = <0...255>	IEC TS 62351-5:2013, 7.2.9.3	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.10		SCS: Status Change Sequence Number Value Range = <0...4294967295> This value shall be equal to the last KSQ sent plus 1.	IEC TS 62351-5:2013, 7.2.9.4	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.11		URL: User Role Value range = <0...65535>	IEC TS 62351-5:2013, 7.2.9.5	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.12		UEI: User Role Expiry Interval Value range = <0...65535>	IEC TS 62351-5:2013, 7.2.9.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.13	S_US_NA_1 ASDU 90 User Status Change (continued)	UNL: User Name Length Value range = <0...65535>	IEC TS 62351-5:2013, 7.2.9.7	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.14		UKL: User Public Key Length Value range = <0...65535> This value shall be 0 (zero) if KCM specifies a symmetric Update Key change method.	IEC TS 62351-5:2013, 7.2.9.8	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.15		CDL: Certification Data Length Value range = <0...65535>	IEC TS 62351-5:2013, 7.2.9.9	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7

No.	Test	Description	Reference	Required
6.3.1.16		UN: User Name Sequence of octets of length specified in UNL	IEC TS 62351-5:2013, 7.2.9.10	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.17		UK: User Public Key Sequence of octets of length specified in UKL This field is shall not be included if KCM specifies a symmetric Update Key change method.	IEC TS 62351-5:2013, 7.2.9.11	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
6.3.1.18		CD: Certification Data Sequence of octets of length specified in CDL This field shall contain valid certificate data provided by the authority without any modification.	IEC TS 62351-5:2013, 7.2.9.12	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
1) IEC TS 60870-5-7 Documentation issue: “S_UC_NA_1” ASDU name is wrongly assigned to both Type ID 88 and Type ID 95. This issue will be corrected in the next revision of IEC TS 60870-5-7.				

6.3.2 Update key maintenance ASDUs

Table 5 – Update key maintenance ASDUs

No.	Test	Description	Reference	Required
6.3.2.1	S_UQ_NA_1 ASDU 91 Update Key Change Request	VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.10	IEC 60870-5-7 PICS 10.6
6.3.2.2		COT: Cause of Transmission Controlling Station values = 16 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.10	IEC 60870-5-7 PICS 10.6
6.3.2.3		KCM: Key Change Method Value range = <0…255>	IEC TS 62351-5:2013, 7.2.9.2	IEC 60870-5-7 PICS 10.6
6.3.2.4		UNL: User Name Length Value range = <0…65535>	IEC TS 62351-5:2013, 7.2.10.3	IEC 60870-5-7 PICS 10.6
6.3.2.5		CCL: Controlling Station Challenge Data Length Value range = <4…65535>	IEC TS 62351-5:2013, 7.2.10.4	IEC 60870-5-7 PICS 10.6
6.3.2.6		UN: User Name Sequence of octets of length specified in UNL	IEC TS 62351-5:2013, 7.2.10.5	IEC 60870-5-7 PICS 10.6
6.3.2.7		CGC: Controlling Station Challenge Data Sequence of octets of length specified in CCL	IEC TS 62351-5:2013, 7.2.10.6	IEC 60870-5-7 PICS 10.6
6.3.2.8	S_UR_NA_1 ASDU 92 Update Key Change Reply	A.1.1.2 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6
6.3.2.9		COT: Cause of Transmission Value = 16	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6
6.3.2.10		KSQ: Key Change Sequence Number Value range = <0…4294967295> This value shall be equal to the last KSQ sent plus 1.	IEC TS 62351-5:2013, 7.2.11.2	IEC 60870-5-7 PICS 10.6

No.	Test	Description	Reference	Required
6.3.2.11		USR: User Number Value range = <1...65535> This value shall be the number assigned to the User Name specified in the last Update Key Change Request received.	IEC TS 62351-5:2013, 7.2.11.3	IEC 60870-5-7 PICS 10.6
6.3.2.12		CDL: Controlled Station Challenge Data Length Value range = <4...65535>	IEC TS 62351-5:2013, 7.2.11.4	IEC 60870-5-7 PICS 10.6
6.3.2.13		CDC: Controlled Station Challenge Data Sequence of octets of length specified in CDL	IEC TS 62351-5:2013, 7.2.11.5	IEC 60870-5-7 PICS 10.6
6.3.2.14	S_UK_NA_1 ASDU 93 Update Key Change - Symmetric	A.1.1.3 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6
6.3.2.15		COT: Cause of Transmission Controlling Station values = 16 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6
6.3.2.16		KSQ: Key Change Sequence Number Value range = <0...4294967295> This value shall be the same of that in the last Update Key Change Reply received.	IEC TS 62351-5:2013, 7.2.12.2	IEC 60870-5-7 PICS 10.6
6.3.2.17		USR: User Number Value range = <1...65535> This value shall be the same of that in the last Update Key Change Reply received.	IEC TS 62351-5:2013, 7.2.12.3	IEC 60870-5-7 PICS 10.6
6.3.2.18		EUL: Encrypted Update Key Length Value range = <16...65535>	IEC TS 62351-5:2013, 7.2.12.4	IEC 60870-5-7 PICS 10.6

No.	Test	Description	Reference	Required
6.3.2.19		EUD: Encrypted Update Key Sequence of octets of length specified in EUL. This field shall contain the correct value according to: - the data included in the EUD calculation, - the encryption algorithm associated to the key change method specified in KCM of the last Update Key Change Request sent - the symmetric key pre-shared between the Authority and the Station.	IEC TS 62351-5:2013, 7.2.12.5	IEC 60870-5-7 PICS 10.6
6.3.2.20		MAC: Message Authentication Code Sequence of octets of length according to the MAC algorithm associated to the key change method specified in KCM of the last Update Key Change Request sent. This field shall contain the correct value according to: - the data included in the MAC calculation, - the MAC algorithm associated to the key change method specified in KCM of the last Update Key Change Request sent, - the new Update Key supplied in this S_UK_NA_1 message and associated to the User specified in USR.	IEC TS 62351-5:2013, 7.2.14.2	IEC 60870-5-7 PICS 10.6
6.3.2.21	S_UA_NA_1 ASDU 94 Update Key Change - Asymmetric	A.1.1.4 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6

No.	Test	Description	Reference	Required
6.3.2.22		COT: Cause of Transmission Controlling Station values = 16 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.11	IEC 60870-5-7 PICS 10.6
6.3.2.23		KSQ: Key Change Sequence Number Value range = <0...4294967295> This value shall be the same of that in the last Update Key Change Reply received.	IEC TS 62351-5:2013, 7.2.12.2	IEC 60870-5-7 PICS 10.6
6.3.2.24		USR: User Number Value range = <1...65535> This value shall be the same of that in the last Update Key Change Reply received.	IEC TS 62351-5:2013, 7.2.12.3	IEC 60870-5-7 PICS 10.6
6.3.2.25		EUL: Encrypted Update Key Length Value range = <16...65535>	IEC TS 62351-5:2013, 7.2.12.4	IEC 60870-5-7 PICS 10.6
6.3.2.26		EUD: Encrypted Update Key Sequence of octets of length specified in EUL. This field shall contain the correct value according to: - the data included in the EUD calculation, - the encryption algorithm associated to the key change method specified in KCM of the last Update Key Change Request sent - the Controlled Station's public key.	IEC TS 62351-5:2013, 7.2.12.5	IEC 60870-5-7 PICS 10.6

No.	Test	Description	Reference	Required
6.3.2.27		DS: Digital Signature Sequence of octets of length according to the digital signature algorithm associated to the Key Change Method specified in KCM of the last Update Key Change Request sent. This field shall contain the correct value according to: - the data included in the Digital Signature calculation, - the signature algorithm associated to the key change method specified in KCM of the last Update Key Change Request sent, - the private key of the User specified in USR, corresponding to the public key supplied in the last User Status Change message sent for the same USR.	IEC TS 62351-5:2013, 7.2.13.2	IEC 60870-5-7 PICS 10.6
6.3.2.28	S_UC_NA_1 ASDU 95 Update Key Change Confirmation	A.1.1.5 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.4	IEC 60870-5-7 PICS 10.6
6.3.2.29	See NOTE (1)	COT: Cause of Transmission Controlled Station values = 16	IEC TS 60870-5-7:2013, 7.3.4	IEC 60870-5-7 PICS 10.6

No.	Test	Description	Reference	Required
6.3.2.30		MAC: Message Authentication Code Sequence of octets of length according to the MAC algorithm associated to the key change method specified in KCM of the last Update Key Change Request received. This field shall contain the correct value according to: - the data included in the MAC calculation, - the MAC algorithm associated to the key change method specified in KCM of the last Update Key Change Request received, - the Update Key supplied in the last Update Key Change message received and associated to the User specified in USR of that message.	IEC TS 62351-5:2013, 7.2.14.2	IEC 60870-5-7 PICS 10.6
1) IEC TS 60870-5-7 Documentation issue: “S_UC_NA_1” ASDU name is wrongly assigned to both Type ID 88 and Type ID 95. This issue will be corrected in the next revision of IEC TS 60870-5-7.				

6.3.3 Session key maintenance ASDUs

Table 6 – Session key maintenance ASDUs

No.	Test	Description	Reference	Required
6.3.3.1	S_KR_NA_1 ASDU 84 Session Key Status Request	VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.4	M
6.3.3.2		COT: Cause of Transmission Controlling Station values = 15 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.4	M
6.3.3.3		USR: User Number Value range = <1…65535>	IEC TS 62351-5:2013, 7.2.4.4	M
6.3.3.4	S_KS_NA_1 ASDU 85 Session Key Status	VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.5	M
6.3.3.5		COT: Cause of Transmission Value = 15	IEC TS 60870-5-7:2013, 7.3.5	M
6.3.3.6		KSQ: Key Change Sequence Number Value range = <0…4294967295> This value shall be equal to the last KSQ sent plus 1.	IEC TS 62351-5:2013, 7.2.6.2	M
6.3.3.7		USR: User Number Value range = <1…65535> This value shall be the same of that in the last Session Key Status Request received.	IEC TS 62351-5:2013, 7.2.6.3	M
6.3.3.8		KWA: Key Wrap Algorithm Values = 1, 2	IEC TS 62351-5:2013, 7.2.6.4	IEC 60870-5-7 PICS 10.4
6.3.3.9		KST: Key Status Value range = <1…4>	IEC TS 62351-5:2013, 7.2.6.5	M

No.	Test	Description	Reference	Required
6.3.3.10		MAL: MAC Algorithm Values = 0, 3, 4, 6 This value shall be 0 if no valid Session Key Change message was previously received (i.e. if there is no Session Key).	IEC TS 62351-5:2013, 7.2.6.6	IEC 60870-5-7 PICS 10.3
6.3.3.11	S_KS_NA_1 ASDU 85 Session Key Status (continued)	KCL: Key Status Challenge Data Length Value range = <8...64>	IEC TS 62351-5:2013, 7.2.6.7 IEC TS 60870-5-7:2013, 7.2.4	M
6.3.3.12		KCD: Key Status Challenge Data Sequence of octets of length specified in KCL	IEC TS 62351-5:2013, 7.2.6.8	M
6.3.3.13		MAC: Message Authentication Code Sequence of octets of length according to the MAC algorithm specified in MAL. If MAL=0 then no MAC is included in this message. This field shall contain the correct value according to: - the data included in the MAC calculation, - the MAC algorithm specified in MAL, - the last session key considered valid, belonging to the User specified in USR.	IEC TS 62351-5:2013, 7.2.6.9	M
6.3.3.14	S_KC_NA_1 ASDU 86 Session Key Change	A.1.1.6 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.6	M
6.3.3.15		COT: Cause of Transmission Controlling Station values = 15 Controlled Station values = 44	IEC TS 60870-5-7:2013, 7.3.6	M

No.	Test	Description	Reference	Required
6.3.3.16		KSQ: Key Change Sequence Number Value range = <0…4294967295> This value shall be the same of that in the last Session Key Status received.	IEC TS 62351-5:2013, 7.2.7.2	M
6.3.3.17		USR: User Number Value Range = <1…65535>	IEC TS 62351-5:2013, 7.2.7.3	M
6.3.3.18		WKL: Wrapped Key Data Length Value Range = <8…1024>	IEC TS 62351-5:2013, 7.2.7.4 IEC TS 60870-5-7:2013, 7.2.4	M
6.3.3.19		WKD: Wrapped Key Data Sequence of octets of length specified in WKL. This field shall contain the correct value according to: - the data included in the WKD calculation, - the key wrap algorithm specified in KWA of the last Session Key Status received, - the Update Key assigned to the User specified in USR.	IEC TS 62351-5:2013, 7.2.7.5	M

6.3.4 Challenge/reply and aggressive mode authentication ASDUs

Table 7 – Challenge/reply and aggressive mode authentication ASDUs

No.	Test	Description	Reference	Required
6.3.4.1	S_CH_NA_1 ASDU 81 Authentication challenge	A.1.1.7 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.1	M
6.3.4.2		COT: Cause of Transmission Controlling Station values = 14 Controlled Station values = 14, 44, 45, 46	IEC TS 60870-5-7:2013, 7.3.1	M
6.3.4.3		CSQ: Challenge Sequence Number Value Range = <0…4294967295> This value shall be calculated as follow: - If the last CSQ sent is greater than or equal to the last CSQ received, this value shall be equal to the last CSQ sent plus 1. - If the last CSQ received is greater than the last CSQ sent, this value shall be equal to the last CSQ received plus 1.	IEC TS 62351-5:2013, 7.2.2.2	M
6.3.4.4		USR: User Number Controlling Station value range = <1…65535> Controlled Station values = 0	IEC TS 62351-5:2013, 7.2.2.3	M
6.3.4.5		MAL: MAC Algorithm Values = 3, 4, 6	IEC TS 62351-5:2013, 7.2.2.4	IEC 60870-5-7 PICS 10.3
6.3.4.6		RSC: Reason for Challenge Value = 1	IEC TS 62351-5:2013, 7.2.2.5	M
6.3.4.7		CLN: Challenge Data Length Value range = <4…64>	IEC TS 62351-5:2013, 7.2.2.6 IEC TS 60870-5-7:2013, 7.2.4	M
6.3.4.8		CHD: Challenge Data Sequence of octets of length specified in CLN	IEC TS 62351-5:2013, 7.2.2.7	M

No.	Test	Description	Reference	Required
6.3.4.9	S_RP_NA_1 ASDU 82 Authentication Reply	A.1.1.8 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.2	M
6.3.4.10		COT: Cause of Transmission Controlling Station values = 14 Controlled Station values = 14, 44, 45, 46	IEC TS 60870-5-7:2013, 7.3.2	M
6.3.4.11		CSQ: Challenge Sequence Number Value range = <0…4294967295> The value shall be the same of that in the last Authentication Challenge received.	IEC TS 62351-5:2013, 7.2.3.2	M
6.3.4.12		USR: User Number Controlling Station value range = <1…65535> Controlled Station values = 1	IEC TS 62351-5:2013, 7.2.3.3	M
6.3.4.13		HLN: MAC Length Value range = <2…64> This field shall contain the correct value according to the MAC algorithm in the MAL field of the last Authentication Challenge received.	IEC TS 62351-5:2013, 7.2.3.4 IEC TS 60870-5-7:2013, 7.2.4	M
6.3.4.14		MAC: Message Authentication Code Sequence of octets of length specified in HLN. This field shall contain the correct value according to - the data included in the MAC calculation, - the MAC algorithm specified in MAL of the last Authentication Challenge received, - the current (valid) session key belonging to the User specified in USR.	IEC TS 62351-5:2013, 7.2.3.5	M

No.	Test	Description	Reference	Required
6.3.4.15	S_AR_NA_1 ASDU 83 Aggressive Mode Authentication Request	A.1.1.9 VSQ: Variable Structure Qualifier SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.3	M
6.3.4.16		COT: Cause of Transmission Controlling Station values = 14 Controlled Station values = 14, 44, 45, 46	IEC TS 60870-5-7:2013, 7.3.3	M
6.3.4.17		CSQ: Challenge Sequence Number Value Range = <0…4294967295> This value shall be calculated as follow: - If the last CSQ sent is greater than or equal to the last CSQ received, this value shall be equal to the last CSQ sent plus 1. - If the last CSQ received is greater than the last CSQ sent, this value shall be equal to the last CSQ received plus 1.	IEC TS 62351-5:2013, 7.2.4.3	M
6.3.4.18		USR: User Number Controlling Station value range = <1…65535> Controlled Station values = 1	IEC TS 62351-5:2013, 7.2.4.4	M

No.	Test	Description	Reference	Required
6.3.4.19		MAC: Message Authentication Code Sequence of octets of length according to the MAC algorithm specified in MAL of the last Authentication Challenge received. This field shall contain the correct value according to - the data included in the MAC calculation, - the MAC algorithm specified in MAL of the Authentication Challenge most recently received, - the current (valid) session key belonging to the User specified in USR.	IEC TS 62351-5:2013, 7.2.4.5	M
6.3.4.20		The base protocol ASDU authenticated by the Aggressive Mode Authentication Request is conformant to the base protocol standard.	IEC 60870-5-101 IEC 60870-5-104	M

6.3.5 Security statistics ASDU

Table 8 – Security statistics ASDU

No.	Test	Description	Reference	Required
6.3.5.1	S_IT_TC_1 ASDU 41 Integrated totals containing time-tagged security statistics	A.1.1.10 VSQ: Variable Structure Qualifier SQ = 0 N = <1…127>	IEC TS 60870-5-7:2013, 7.3.15	M
6.3.5.2		COT: Cause of Transmission Values = 3, 37, 38, 39, 40, 41, 44, 45, 46	IEC TS 60870-5-7:2013, 7.3.15	M
6.3.5.3		IOA: Information Object Address The value of this field shall be set according to one of the statistic information object addresses defined in the PICS.	IEC TS 60870-5-7:2013, 7.3.15 IEC TS 60870-5-7:2013, 10.9	M
6.3.5.4		AID: Association ID Values: <0…65535>	IEC TS 60870-5-7:2013, 7.3.15	M
6.3.5.5		BCR: Binary Counter Reading This field shall contain the value of the statistic counter addressed by the IOA (Information Object Address).	IEC TS 60870-5-7:2013, 7.3.15	M
6.3.5.6		CP56Time2a: Seven octets binary time	IEC TS 60870-5-7:2013, 7.3.15	M

7 Verification of procedures

7.1 General

The purpose of this clause is to verify that the DUT correctly implements the security extension procedures, each with the correct set of messages, as specified in IEC TS 60870-5-7.

For profiles including TCP/IP, prior to execute these procedures, the following initial conditions shall be satisfied:

a) The TCP/IP connection is established and the TLS session is also successfully established.

7.2 User management

7.2.1 General

This procedure shall be performed whenever and only when the Central Authority change the status of a User on Controlled Station via the Controlling Station.

This procedure shall be performed if Users can be configured using the affected protocol and only when the Central Authority change the status of a User (on Controlled Station via the Controlling Station). Consequently, the Update keys can be changed by means of the protocol (i.e. they are not pre-shared).

After the Station start-up, if no User has been previously added (or pre-configured), User Management shall be the first procedure to be performed. In this condition, the Controlling Station does not start any secure procedure to the Controlled Station until the Central Authority initiates the procedure to add users. It is expected that the Central Authority proceeds to add Users by the Controlling Station, starting from the Default User.

The recommended methods and protocols to be used to forward certification data from the central authority to the controlling station are defined in IEC 62351-9 and are out of scope of this document. The controlling station is responsible for initiating the user management procedure to the controlled station.

7.2.2 Controlling station

7.2.2.1 Normal procedure test cases

Table 9 – User management: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.2.2.1.1	The station receives from the authority some new signed Certification Data for a particular user. Controlling and Controlled Stations are configured to use a **symmetric** Update Key Change method.	Send S_US_NA_1 for that user specifying a symmetric Update Key change method in KCM. Initiates the Update Key Maintenance - symmetric - procedure for the same user according to the Update Key change method specified in KCM.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 62351-5:2013, 7.3.5.5 IEC TS 62351-5:2013, 7.3.5.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
7.2.2.1.2	The station receives from the authority some new signed Certification Data for a particular user. Controlling and Controlled Stations are configured to use an **asymmetric** Update Key Change method.	Send S_US_NA_1 for that user specifying an asymmetric Update Key change method in KCM. Initiates the Update Key Maintenance - asymmetric - procedure for the same user according to the Update Key change method specified in KCM.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 62351-5:2013, 7.3.5.5 IEC TS 62351-5:2013, 7.3.5.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
7.2.2.1.3	The station receives from the authority a new X.509 Certificate (with 62351-8 Role extension for a particular user). Controlling and Controlled Stations are configured to use an **asymmetric** Update Key Change method.	Send S_UC_NA_1 for that user specifying an asymmetric Update Key change method in KCM. Initiates the Update Key Maintenance - asymmetric - procedure for the same user according to the Update Key change method specified in KCM.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 62351-5:2013, 7.3.5.5 IEC TS 62351-5:2013, 7.3.5.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.7
7.2.2.1.4	Upon sending S_US_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received.	See NOTE (1)	IEC 60870-5-7 PICS 10.7
7.2.2.1.5	Upon sending S_UC_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received.	See NOTE (1)	IEC 60870-5-7 PICS 10.7

1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a User Status Change message or a User Certificate message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.

7.2.2.2 Resiliency procedure test cases

Table 10 – User management: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.2.2.2.1	Upon sending S_US_NA_1: Reception of a S_ERR_NA_1	Increment the Failed Update Key Change statistic. Log the Error Message Received.	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.7
7.2.2.2.2	Upon sending S_US_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.7
7.2.2.2.3	Upon sending S_US_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.7
7.2.2.2.4	Upon sending S_UC_NA_1: Reception of a S_ERR_NA_1	Increment the Failed Update Key Change statistic. Log the Error Message Received.	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.7
7.2.2.2.5	Upon sending S_UC_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.7
7.2.2.2.6	Upon sending S_UC_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.7
7.2.2.2.7	Reception of an unexpected ASDU (unsolicited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		IEC 60870-5-7 PICS 10.7
1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a User Status Change message or a User Certificate message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.				

7.2.3 Controlled station

7.2.3.1 Normal procedure test cases

Table 11 – User management: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.2.3.1.1	Reception of a valid S_US_NA_1 to ADD a new User Name (not previously created in the Controlled Station).	Assign a new (not already used) User Number (USR) to the User Name specified in the message received. Store the Certification Data locally for the USR.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.1.2	Reception of a valid S_US_NA_1 to CHANGE the status of an existing User Name (previously created in the Controlled Station).	Store the Certification Data locally for the USR.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.1.3	Reception of a valid S_US_NA_1 to DELETE an existing User Name (previously created in the Controlled Station).	Remove the Certification Data stored locally for the USR. Free the User Number (USR)	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.1.4	Reception of a valid S_UC_NA_1 to ADD a new User Name (not previously created in the Controlled Station).	Assign a new (not already used) User Number (USR) to the User Name specified in the message received. Store the Certification Data locally for the USR.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.1.5	Reception of a valid S_UC_NA_1 to CHANGE the status of an existing User Name (previously created in the Controlled Station).	Store the Certification Data locally for the USR.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.1.6	Reception of a valid S_UC_NA_1 to DELETE an existing User Name (previously created in the Controlled Station).	Remove the Certification Data stored locally for the USR. Free the User Number (USR)	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7

7.2.3.2 Resiliency test cases

Table 12 – User management: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.2.3.2.1	Reception of a valid S_US_NA_1 to ADD an already existing User Name (previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.2	Reception of a valid S_US_NA_1 to CHANGE the status of a Not existing User Name (not previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5
7.2.3.2.3	Reception of a valid S_US_NA_1 to DELETE a NOT existing User Name (not previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5

No.	Test	Action	Reference	Required
7.2.3.2.4	Reception of a valid S_US_NA_1 with a unsupported Update Key Change method in KCM	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 8 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5
7.2.3.2.5	Reception of a valid S_US_NA_1 with a unrecognized Operation in OPR	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.6	Reception of a valid S_US_NA_1 with a unrecognized User Role in URL	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.7	Reception of a valid S_US_NA_1 with a User Role Expiry Interval (UEI) equal to 0 (zero)	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.8	Reception of a S_US_NA_1 with a NOT valid Certification Data (one of the values in the message fields does not match the same value in the Certification Data)	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 10 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5

No.	Test	Action	Reference	Required
7.2.3.2.9	Reception of a S_US_NA_1 with a NOT valid Certification Data signature	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 9 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5
7.2.3.2.10	Reception of a valid S_UC_NA_1 to ADD an already existing User Name (previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.11	Reception of a valid S_UC_NA_1 to CHANGE the status of a Not existing User Name (not previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5
7.2.3.2.12	Reception of a valid S_UC_NA_1 to DELETE a NOT existing User Name (not previously created in the Controlled Station).	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5

No.	Test	Action	Reference	Required
7.2.3.2.13	Reception of a valid S_UC_NA_1 specifying an unsupported Update Key Change method in KCM	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 8 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5
7.2.3.2.14	Reception of a valid S_UC_NA_1 specifying a Symmetric Update Key Change method in KCM	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.15	Reception of a valid S_UC_NA_1 with a unrecognized Operation in in the X.509 Certificate RBAC extension	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.16	Reception of a valid S_UC_NA_1 with a unrecognized User Role in the X.509 Certificate RBAC extension	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7
7.2.3.2.17	Reception of a valid S_UC_NA_1 with a Not valid AOR in the X.509 Certificate RBAC extension (i.e. AOR is not that the Controlled Station belongs to)	Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 7 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.5	IEC 60870-5-7 PICS 10.7 IEC 60870-5-7 PICS 10.5

7.3 Update key maintenance - Symmetric

7.3.1 General

This procedure is performed if both stations agreed to use the symmetric update key change method. It shall be performed after a successfully completed user management (user status change) procedure and executed for the same User (USR) involved in the last user status change. The controlling station is responsible for initiating the update key maintenance procedure.

Prior to executing this procedure, the following initial conditions shall be satisfied:

a) At least one user (USR) was successfully added on the stations. The default user (USR 1) shall always be added first.

Also, the following requirements shall be satisfied:

b) This procedure shall be performed for each User added, whenever a triggering condition in Table 13 occurs. All triggering conditions listed in Table 13 shall be verified for each User added.

7.3.2 Controlling station

7.3.2.1 Triggering conditions

Table 13 – Update key maintenance – Symmetric: Controlling station triggering conditions

No.	Test	Description	Reference	Required
7.3.2.1.1	User Management procedure was successfully executed for a USR specifying a **symmetric** Update Key Change method.	The Station initiates the Symmetric Update Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 7.3.5.6	IEC 60870-5-7 PICS 10.6

7.3.2.2 Normal procedure test cases

Table 14 – Update key maintenance – Symmetric: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.3.2.2.1	Start Symmetric Update Key Maintenance procedure	Send S_UQ_NA_1 specifying a symmetric Update Key change method in KCM Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.2.2	Upon sending S_UQ_NA_1: Reception of a valid S_UR_NA_1	Stop Reply Timer. Send S_UK_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.2.3	Upon sending S_UK_NA_1: Reception of a valid S_UC_NA_1	Stop Reply Timer. Reset the Reply Timeouts Statistic Increment the Successful Authentication statistic Increment the Update Key Changes statistic Store and begin to use the new Update Key transmitted in the last S_UK_NA_1 sent.	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.2.4	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.2.5	Upon sending S_UK_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received.	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.2.6	Upon sending S_UQ_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.2.7	Upon sending S_UK_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a Update Key Change Request or a Update Key Change message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.				

7.3.2.3 Resiliency test cases

Table 15 – Update key maintenance – Symmetric: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.3.2.3.1	Upon sending S_UQ_NA_1: Reply timeout expired.	IF Reply Timeouts <= Max Reply Timeouts - Increment Reply Timeout statistic - Send S_UQ_NA_1 - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.3.2		IF Reply Timeouts > Max Reply Timeouts - Increment Failed Update Key Change statistic - Reset Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.3.3	Upon sending S_UQ_NA_1: Reception an S_ER_NA_1	Log the Error Message received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.3.4	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.3.5	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.3.6	Upon sending S_UK_NA_1: Reply timeout expired	IF Reply Timeouts <= Max Reply Timeouts - Increment Reply Timeout statistic - Send S_UK_NA_1 - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.3.7		IF Reply Timeouts > Max Reply Timeouts - Increment Failed Update Key Change statistic - Reset Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6

No.	Test	Action	Reference	Required
7.3.2.3.8	Upon sending S_UK_NA_1: Reception an S_ER_NA_1	Log the Error Message received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.3.2.3.9	Upon sending S_UK_NA_1: Reception an S_UC_NA_1 with a NOT valid MAC	Stop Reply Timer Discard the message Increment the Message Discarded statistic Increment the Authentication Failure statistic Increment the Failed Update Key Change statistic IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.3.2.3.10	Upon sending S_UK_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.3.11	Upon sending S_UK_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.3.2.3.12	Reception of an unexpected ASDU (unsolicited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		IEC 60870-5-7 PICS 10.6

1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a Update Key Change Request or a Update Key Change message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.

7.3.3 Controlled station

7.3.3.1 Normal procedure test cases

Table 16 – Update key maintenance – Symmetric: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.3.3.1.1	Reception of a S_UQ_NA_1 for a valid User Name (previously created in the Controlled Station)	Send S_UR_NA_1 with USR assigned to the User Name.	IEC TS 62351-5:2013, 6.3.4 Fig.8 IEC TS 62351-5:2013, 7.2.11	IEC 60870-5-7 PICS 10.6
7.3.3.1.2	Reception of a valid S_UK_NA_1	Store and begin to use the new Update Key received Send S_UC_NA_1	IEC TS 62351-5:2013, 6.3.4 Fig.8 IEC TS 62351-5:2013, 7.2.14	IEC 60870-5-7 PICS 10.6

7.3.3.2 Resiliency test cases

Table 17 – Update key maintenance – Symmetric: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.3.3.2.1	Reception of a S_UQ_NA_1 for a NOT valid User Name (not created in the Controlled Station)	Discard the ASDU received. Increment the Discarded Message Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.3.3.2.2	Reception of a S_UQ_NA_1 with a NOT valid Key Change Method (KCM)	Discard the ASDU received. Increment the Discarded Message Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 8 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.3.3.2.3	Reception of a S_UK_NA_1 with KSQ not matching to that in the last S_UR_NA_1 sent.	Discard the ASDU received. Increment Discarded Message Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6
7.3.3.2.4	Reception of a S_UK_NA_1 with USR not matching to that in the last S_UR_NA_1 sent.	Discard the ASDU received. Increment Discarded Message Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6
7.3.3.2.5	Reception of a S_UK_NA_1 with a valid MAC and a NOT valid Encrypted Update Key Data (EUD).	Discard the ASDU received. Increment the Discarded Message Statistic. Increment the Authentication Failures Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6

No.	Test	Action	Reference	Required
7.3.3.2.6	Reception of a S_UK_NA_1 with a NOT valid MAC	Discard the ASDU received. Increment the Discarded Message Statistic. Increment the Authentication Failures Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5

7.4 Update key maintenance – Asymmetric

7.4.1 General

This procedure is performed if both stations agreed to use the Asymmetric Update Key Change method. It shall be performed after a successfully completed User Management (User Status Change) procedure, and executed for the same User (USR) involved in the last User Status Change. The Controlling Station is responsible for initiating the Update Key Maintenance procedure.

Prior to executing this procedure, the following initial conditions shall be satisfied:

a) At least one user (USR) was successfully added on the stations. The default user (USR 1) shall always be added first.

Also, the following requirements shall be satisfied:

b) This procedure shall be performed for each user added, whenever a triggering condition in Table 18 occurs. All triggering conditions listed in Table 18 shall be verified for each user added.

7.4.2 Controlling station

7.4.2.1 Triggering conditions

Table 18 – Update key maintenance – Asymmetric: Controlling station triggering conditions

No.	Test	Description	Reference	Required
7.4.2.1.1	User Management procedure was successfully executed for a USR specifying an Asymmetric Update Key Change method	The Station initiates the Asymmetric Update Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 7.3.5.6	IEC 60870-5-7 PICS 10.6
7.4.2.1.2	Organization's security policy requests to perform Update Key Maintenance for a USR	The Station initiates the Asymmetric Update Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 6.2.7.3	IEC 60870-5-7 PICS 10.6

7.4.2.2 Normal procedure test cases

Table 19 – Update key maintenance – Asymmetric: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.4.2.2.1	Start Update Key Maintenance procedure	Send S_UQ_NA_1 specifying an asymmetric Update Key change method in KCM Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.2.2	Upon sending S_UQ_NA_1: Reception of a valid S_UR_NA_1	Stop Reply Timer. Generate and encrypt a new Update Key Send S_UA_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.2.3	Upon sending S_UA_NA_1: Reception of a valid S_UC_NA_1	Stop Reply Timer. Reset the Reply Timeouts Statistic Increment the Successful Authentication statistic Increment the Update Key Changes statistic Store and begin to use the new Update Key transmitted in the last S_UA_NA_1 sent.	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.2.4	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.4.2.2.5	Upon sending S_UA_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.4.2.3.6	Upon sending S_UQ_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.7	Upon sending S_UA_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a Update Key Change Request message or a Update Key Change message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.				

7.4.2.3 Resiliency test cases

Table 20 – Update key maintenance – Asymmetric: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.4.2.3.1	Upon sending S_UQ_NA_1: Reply timeout expired.	IF Reply Timeouts <= Max Reply Timeouts - Increment Reply Timeout statistic - Send S_UQ_NA_1 - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.2		IF Reply Timeouts > Max Reply Timeouts - Increment Failed Update Key Change statistic - Reset Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.3	Upon sending S_UQ_NA_1: Reception an S_ER_NA_1	Log the Error Message received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.4	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.4.2.3.5	Upon sending S_UQ_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.4.2.3.6	Upon sending S_UA_NA_1: Reply timeout expired	IF Reply Timeouts <= Max Reply Timeouts - Increment Reply Timeout statistic - Send S_UA_NA_1 - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6

No.	Test	Action	Reference	Required
7.4.2.3.7		IF Reply Timeouts > Max Reply Timeouts - Increment Failed Update Key Change statistic - Reset Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.8	Upon sending S_UA_NA_1: Reception an S_ER_NA_1	Log the Error Message received	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.4.2.3.9	Upon sending S_UA_NA_1: Reception an S_UA_NA_1 with a NOT valid MAC	Stop Reply Timer Discard the message Increment the Message Discarded statistic Increment the Authentication Failure statistic Increment the Failed Update Key Change statistic IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.4.2.3.10	Upon sending S_UA_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6
7.4.2.3.11	Upon sending S_UA_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message received Increment the Messages Discarded statistic Increment the Authentication Failures statistic	See NOTE (1)	IEC 60870-5-7 PICS 10.6

No.	Test	Action	Reference	Required
7.4.2.3.12	Reception of an unexpected ASDU (unsolicited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		IEC 60870-5-7 PICS 10.6
1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a User Status Change message or a User Certificate message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.				

7.4.3 Controlled station

7.4.3.1 Normal procedure test cases

Table 21 – Update key maintenance – Asymmetric: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.4.3.1.1	Reception of a S_UQ_NA_1 for a valid User Name (previously created in the Controlled Station)	Send S_UR_NA_1 with USR assigned to the User Name.	IEC TS 62351-5:2013, 6.3.4 Fig.8 IEC TS 62351-5:2013, 7.2.11	IEC 60870-5-7 PICS 10.6
7.4.3.1.2	Reception of a valid S_UA_NA_1	Store and begin to use the new Update Key received Send S_UC_NA_1	IEC TS 62351-5:2013, 6.3.4 Fig.8 IEC TS 62351-5:2013, 7.2.14	IEC 60870-5-7 PICS 10.6

7.4.3.2 Resiliency test cases

Table 22 – Update key maintenance – Asymmetric: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.4.3.2.1	Reception of a S_UQ_NA_1 for a NOT valid User Name (not created in the Controlled Station)	Discard the ASDU received. Increment the Discarded Message Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 11 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.4.3.2.2	Reception of a S_UQ_NA_1 with a NOT valid Key Change Method (KCM)	Discard the ASDU received. Increment the Discarded Message Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 8 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
7.4.3.2.3	Reception of a S_UA_NA_1 with KSQ not matching to that in the last S_UR_NA_1 sent.	Discard the ASDU received. Increment Discarded Message Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6
7.4.3.2.4	Reception of a S_UA_NA_1 with USR not matching to that in the last S_UR_NA_1 sent.	Discard the ASDU received. Increment Discarded Message Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6
7.4.3.2.5	Reception of a S_UA_NA_1 with a valid Digital Signature and a NOT valid Encrypted Update Key Data (EUD).	Discard the ASDU received. Increment the Discarded Message Statistic. Increment the Authentication Failures Statistic.	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6

No.	Test	Action	Reference	Required
7.4.3.2.6	Reception of a S_UA_NA_1 with a NOT valid Digital Signature	Discard the ASDU received. Increment the Discarded Message Statistic. Increment the Authentication Failures Statistic. IF Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 9 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.6	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5

7.5 Session key maintenance

7.5.1 General

This procedure shall be performed whenever one of the conditions defined in Table 23 occurs and it shall be executed for all users preconfigured/added on controlled station. The controlling station is responsible for initiating the session key maintenance procedure.

Prior to executing this procedure, the following initial conditions shall be satisfied:

a) At least one user (USR) and its own update key was successfully added (or preconfigured) on the stations. The default user (USR 1) with its own update key shall always be added (or preconfigured).

Also, the following requirements shall be satisfied:

b) This procedure shall be performed for each User added (or preconfigured) and owning the update key, whenever a triggering condition in Table 23 occurs. All triggering conditions listed in Table 23 shall be verified for each User added (or preconfigured).

7.5.2 Controlling station

7.5.2.1 Triggering conditions

Table 23 – Session key maintenance: Controlling station triggering conditions

No.	Test	Description	Reference	Required
7.5.2.1.1	Connection establishment	Upon the connection is established, the Station executes the Session Key maintenance procedure as first operation for each User (USR) added (or pre-configured), starting from USR 1 (Default User).	IEC TS 62351-5:2013, 6.3.4	M
7.5.2.1.2	Update Key Change procedure was successfully performed for a USR	The Station immediately initiates the Session Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 7.3.5.7 Table 33	IEC 60870-5-7 PICS 10.6
7.5.2.1.3	Session Key Change Timeout expires for a USR	Initiates the Session Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.2.1.4	Session Key Change Count exceeded for a USR	Initiates the Session Key Maintenance procedure for the same USR.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.2.1.5	Reception of End of Initialization ASDU (M_EI_NA_1).	IF Rekeys Due to Restarts <= Max Rekeys Due to Restarts: - Process the ASDU. - Increment the Rekeys Due to Restart statistic - Reset Reply Timeouts statistic - The Station executes the Session Key maintenance procedure as first operation for each User (USR) configured, starting from USR 1 (default user).	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.2.1.6		IF Rekeys Due to Restarts > Max Rekeys Due to Restarts: - Discard the ASDU received - Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5	M

7.5.2.2 Normal procedure test cases

Table 24 – Session key maintenance: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.5.2.2.1	Station initiates the Session Key Change procedure	Send S_KR_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.2.2	Upon sending S_KR_NA_1: reception a S_KS_NA_1 with key status <> OK	Generate new Session Key Send S_KC_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.2.3	Upon sending S_KR_NA_1: reception a S_KS_NA_1 with key status = OK and valid MAC	Generate new Session Key Send S_KC_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.2.4	Upon sending S_KC_NA_1: reception of a S_KS_NA_1 with key status = OK and valid MAC	Stop Reply Timer. Reset Reply Timeouts Statistic. Reset Rekeys due to Restart Statistic. Reset Authentication Failure Statistic. Store and use the new Session Key transmitted in the last S_KC_NA_1 sent. Start Session Key Change Timer. Initiates the Challenge/Reply Authentication procedure for the user specified in USR.	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.2.5	Upon sending S_KR_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received.	See NOTE (1)	M
7.5.2.2.6	Upon sending S_KC_NA_1: Reception of a S_AR_NA_1 with valid MAC and while current Session Key is valid	Process the ASDU received.	See NOTE (1)	M
7.5.2.2.7	Upon sending S_KR_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.2.8	Upon sending S_KC_NA_1: Reception of a Non-Critical ASDU	Process the ASDU received	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
1) In TCP/IP connections or in serial point-to-point connections, while the Controlling Station sends a Session Key Status Request message or a Session Key Change message, the Controlled Station could have already sent an Aggressive Mode Request. In this case, if the Default user session keys are valid, the Controlling Station shall accept and process the Aggressive Mode Request received.				

7.5.2.3 Resiliency test cases

Table 25 – Session key maintenance: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.5.2.3.1	Upon sending S_KR_NA_1: reception of a S_KS_NA_1 with key status = OK and a NOT valid MAC.	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.2	Upon sending S_KR_NA_1: reception of a S_KS_NA_1 with MAC Algorithm (MAL) not supported.	If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 5 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.3	Upon sending S_KR_NA_1: reception of a S_KS_NA_1 with Key Wrap Algorithm (KWA) not supported.	If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 6 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.4	Upon sending S_KR_NA_1: reception a S_KS_NA_1 for a different USR.	Discard the message Increment the Messages Discarded Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.5	Upon sending S_KR_NA_1: Reply Timeout expired	IF Reply Timeouts <= Max Reply Timeouts: - Increments Reply Timeouts Statistic - Send S_KR_NA_1. - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M

No.	Test	Action	Reference	Required
7.5.2.3.6		IF Reply Timeouts > Max Reply Timeouts: - Increment Failed Session Key Change Statistic - Reset Reply Timeouts Statistic - Start Session Key Change Timer. - Start Session Key change procedure for a different USR (if needed).	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.7	Upon sending S_KR_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.8	Upon sending S_KR_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.9	Upon sending S_KC_NA_1: reception of a S_KS_NA_1 with key status = OK and a NOT valid MAC.	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.10	Upon sending S_KC_NA_1: reception of a S_KS_NA_1 with Key Status <> OK	Discard the message Increment the Messages Discarded Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.11	Upon sending S_KC_NA_1: reception a S_KS_NA_1 for a different USR.	Discard the message Increment the Messages Discarded Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.12	Upon sending S_KC_NA_1: Reply Timeout	IF Reply Timeouts <= Max Reply Timeouts - Increments Reply Timeouts Statistic - Send S_KR_NA_1. - Start Reply Timer	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M

No.	Test	Action	Reference	Required
7.5.2.3.13		IF Reply Timeouts > Max Reply Timeouts - Increment Failed Session Key Change Statistic - Reset Reply Timeouts Statistic - Start Session Key Change Timer. - Start Session Key change procedure for a different USR (if needed).	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.14	Upon sending S_KC_NA_1: Reception of a S_AR_NA_1 with a NOT valid MAC and while current Session Key is valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.15	Upon sending S_KC_NA_1: Reception of a S_AR_NA_1 while current Session Key is NOT valid	Discard the message Increment the Messages Discarded Statistic Increment the Authentication Failure Statistic	IEC TS 62351-5:2013, 7.3.5.7 Table 32	M
7.5.2.3.16	Reception of an unexpected ASDU type (unsolicited or unexpected in this procedure).	Discard the message Increment the Discarded Messages statistic Increment the Unexpected Messages statistic		M

7.5.3 Controlled station

7.5.3.1 Conditions invalidating the session key status

Table 26 – Session key maintenance: Controlled station invalidating session key

No.	Test	Action	Reference	Required
7.5.3.1.1	Station Reinitialization	Set Session Key status to NOT_INIT for all USR	IEC TS 62351-5:2013, 7.2.6.5, 7.3.6.2	M
7.5.3.1.2	Station Disconnection	Set Session Key status to COMM_FAIL if current Session Key Status <> NOT_INIT for all USR	IEC TS 62351-5:2013, 7.2.6.5, 7.3.3.5 Table 30	M
7.5.3.1.3	Expected Session Key Change Timeout expired for a USR.	Set Session Key Status to NOT_INIT for that USR	IEC TS 62351-5:2013, 7.2.6.5, 7.3.3.5 Table 30	M
7.5.3.1.4	Expected Session Key Change Count exceeded for a USR.	Set Session Key Status to NOT_INIT for that USR	IEC TS 62351-5:2013, 7.2.6.5, 7.3.3.5 Table 30	M

7.5.3.2 Normal procedure test cases

Table 27 – Session key maintenance: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.5.3.2.1	Reception of a S_KR_NA_1 for a valid USR (previously created in the Controlled Station)	Send S_KS_NA_1 with the current Session Key Status.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.3.2.2	Reception of a S_KC_NA_1 for a valid USR (previously created in the Controlled Station)	Stop sending S_AR_NA_1 and Non-Critical ASDUs Reset Authentication Failures Statistic. Store and use new Session Key received. Set Session Key Status = OK. Send S_KS_NA_1 with the new key status. Start Expected Session Key Change Timer.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

7.5.3.3 Resiliency test cases

Table 28 – Session key maintenance: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.5.3.3.1	Reception of a S_KR_NA_1 for a NOT valid USR (not created in the Controlled Station)	Discard the ASDU received. Increment the Discarded Message Statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.3.3.2	Reception of a S_KC_NA_1 with a NOT valid WKD.	Discard the ASDU received. Increment the Discarded Message Statistic. Increment the Authentication Failures Statistic. Set the Session Key status to AUTH_FAIL Send S_KS_NA_1 with the new key status.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.5.3.3.3	Reception of a S_KC_NA_1 with USR not matching to that in the last S_KS_NA_1 sent.	Discard the ASDU received. Increment Discarded Message Statistic.		M

7.6 Challenge/reply authentication

7.6.1 General

This procedure shall take place immediately after a successfully completed session key maintenance procedure and it shall be executed for the same user (USR) involved in the last session key change. The procedure tested in this subclause allows the DUT to enter in aggressive mode (the normal method of data authentication). The controlling station is responsible for initiating the challenge/reply authentication.

The following requirements shall be satisfied:

a) The test procedure defined in this subclause shall be performed at least once for each user added (or preconfigured) and owning the update key, whenever a triggering condition in Table 29 occurs. All triggering conditions listed in Table 29 shall be verified for each user added (or preconfigured).

b) The challenge/reply authentication shall be performed by sending the base protocol C_TS_NA_1 or C_TS_TA_1 as critical ASDU (IEC TS 60870-5-7:2013, 8.2).

7.6.2 Controlling station

7.6.2.1 Triggering conditions

Table 29 – Challenge/reply authentication: Controlling station triggering conditions

No.	Test	Description	Reference	Required
7.6.2.1.1	Session Key Maintenance successfully executed for a USR	The Station immediately initiates the Challenge/Reply Authentication procedure for the same USR.	IEC TS 60870-5-7:2013, 8.2	M

7.6.2.2 Normal procedure test cases

Table 30 – Challenge/reply authentication: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.6.2.2.1	Start Challenge/Reply Authentication procedure	Send a Critical ASDU Increment the Critical Messages Sent statistic. Start Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.2.2.2	Upon sending a Critical ASDU: Reception of a valid S_CH_NA_1	Stop Reply Timer Send S_RP_NA_1 Start Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.2.2.3	Upon sending a S_RP_NA_1: Reception of a Critical ASDU	Increment the Critical Messages Received statistic. Send S_CH_NA_1 Starts Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.2.2.4	Upon sending S_CH_NA_1: Reception of a valid S_RP_NA_1	Stop Reply Timer. Reset the Reply Timeouts Statistic. Increment the Successful Authentications statistic Process the Critical ASDU pending authentication. Start to send Critical ASDU using Aggressive Mode Request.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.2.2.5	Execution of base protocol procedure	The DUT executes the base protocol procedure according to the critical ASDU used in Challenge/Reply authentication as specified in IEC 60870-5-101 / IEC 60870-5-104.	IEC 60870-5-101 IEC 60870-5-104	M

7.6.2.3 Resiliency test cases

Table 31 – Challenge/reply authentication: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.6.2.3.1	Upon sending a Critical ASDU: Reception of a S_CH_NA_1 with USR <> 0 (zero)	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.2	Upon sending a Critical ASDU: Reception of a S_CH_NA_1 with unrecognized RSC	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.3	Upon sending a Critical ASDU: Reception of a S_CH_NA_1 with unrecognized or unsupported MAL	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.4		If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 5 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5
7.6.2.3.5	Upon sending a Critical ASDU: Reply Timeout expired	If Reply Timeouts <= Max Reply Timeouts: - Increments the Reply Timeouts statistic - Send a Critical ASDU - Start Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.6		If Reply Timeouts > Max Reply Timeouts: - Reset the Reply Timeouts statistic - Initiate the Session Key Change procedure	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.2.3.7	Upon sending a Critical ASDU: Reception of a Critical ASDU	Increment the Critical Messages Received statistic. Discard the Critical ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.8	Reception of an unexpected S_CH_NA_1 (No Critical ASDU was sent)	Increment the Unexpected Messages statistic Discard the message Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.9	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with USR <> 1 (Default)	Discard ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.10	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with a NOT valid MAC	Stop Reply Timer. Reset the Reply Timeouts statistic. Discard the Critical ASDU pending authentication. Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.11		If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5
7.6.2.3.12		If Authentication Failures <= Max Authentication Failures: - Increment the Authentication Failures statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.2.3.13		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys <= Max Authentication Rekeys: - Reset the Authentication Failures statistic - Increment the Authentication Rekeys statistic - Initiate the Session Key Change procedure	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.14		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys > Max Authentication Rekeys: - Reset the Authentication Failures statistic - If operating over TCP/IP: Close Connection	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.15	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with CSQ not matching to that in the last S_CH_NA_1 sent.	Discard ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.16	Upon sending S_CH_NA_1: Reception of a S_ER_NA_1.	Stop Reply Timer Reset Reply Timeouts statistic Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic. Increment the Error Messages Received statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.17	Upon sending S_CH_NA_1: Reception of a Critical ASDU.	Increment the Critical Messages Received statistic. Discard the Critical ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.2.3.18	Upon sending S_CH_NA_1: Reply Timeout expired	Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.19		If Reply Timeouts <= Max Reply Timeouts - Increments the Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.20		If Reply Timeouts > Max Reply Timeouts - Reset Reply Timeouts statistic - Initiate the Session Key Maintenance procedure	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.2.3.21	Reception of an unexpected ASDU (unsolicited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		M

7.6.3 Controlled station

7.6.3.1 Normal procedure test cases

Table 32 – Challenge/reply authentication: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.6.3.1.1	Reception of a Critical ASDU	Send S_CH_NA_1 Starts Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.3.1.2	Upon sending S_CH_NA_1: Reception of a valid S_RP_NA_1	Stop Reply Timer. Reset Reply Timeouts statistic. Increment the Successful Authentication statistic Process the Critical ASDU pending authentication.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.3.1.3	Induce a challenge from Controlling Station	Send a Critical ASDU Start Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.3.1.4	Upon sending Critical ASDU: Reception of a valid S_CH_NA_1	Stop Reply Timer Send S_RP_NA_1 Send next Critical ASDUs through the Aggressive Mode Authentication procedure.	IEC TS 62351-5:2013, 7.3.3.5 Table 30 IEC TS 60870-5-7:2013, 8.2	M
7.6.3.1.5	Execution of base protocol procedure	While executing the Challenge Reply Authentication, the DUT performs the base protocol procedure according the critical ASDU sent/received as specified in IEC 60870-5-101 / IEC 60870-5-104.	IEC 60870-5-101 IEC 60870-5-104	M

7.6.3.2 Resiliency test cases

Table 33 – Challenge/reply authentication: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.6.3.2.1	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with a NOT valid USR.	Discard ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.2	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with a NOT valid MAC	Stop Reply Timer. Reset Reply Timeouts statistic. Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.3		If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5
7.6.3.2.4		If Authentication Failures <= Max Authentication Failures: - Increment the Authentication Failure statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.5		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys <= Max Authentication Rekeys: - Reset the Authentication Failures statistic - Increment the Authentication Rekeys statistic - Set the Session Key Status to AUTH_FAIL	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.3.2.6		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys > Max Authentication Rekeys: - Reset the Authentication Failures statistic - If operating over TCP/IP: Close Connection	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.7	Upon sending S_CH_NA_1: Reception of a S_RP_NA_1 with CSQ not matching to that in the last S_CH_NA_1 sent.	Discard ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.8	Upon sending S_CH_NA_1: Reception of a Critical ASDU.	Increment the Critical Messages Received statistic. Discard the Critical ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.9	Upon sending S_CH_NA_1: Reception S_ER_NA_1.	Stop Reply Timer Reset Max Reply Timeouts statistics Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic. Increment the Error Messages Received statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.10	Upon sending S_CH_NA_1: Reply Timeout expired	Stop Reply Timer Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.11		If Reply Timeouts <= Max Reply Timeouts: - Increment Reply Timeouts statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.3.2.12		If Reply Timeouts statistic > Max Reply Timeouts: - Reset Reply Timeouts statistic - Set Session Key Status to COMM_FAIL	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.13	Upon sending Critical ASDU: Reception of a S_CH_NA_1 with USR <> 1 (default)	Discard ASDU received. Increment Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.14	Upon sending Critical ASDU: Reception of a S_CH_NA_1 with unrecognized RSC	Discard ASDU received. Increment Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.15	Upon sending Critical ASDU: Reception of a S_CH_NA_1 with unrecognized or unsupported MAL	Discard ASDU received. Increment Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.16		If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 5 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5
7.6.3.2.17	Upon sending Critical ASDU: Reply Timeout expired	If Reply Timeouts statistic <= Max Reply Timeouts: - Increments Reply Timeouts statistic - Send a Critical ASDU - Start Reply Timer	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.18		If Reply Timeouts statistic > Max Reply Timeouts: - Reset Reply Timeouts statistic - Set Session Key Status to COMM_FAIL	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.6.3.2.19	Upon sending Critical ASDU: Reception of a Critical ASDU	Increment the Critical Messages Received statistic. Discard the Critical ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.6.3.2.20	Reception of an unexpected ASDU (unsollecited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		M

7.7 Aggressive mode authentication

7.7.1 General

This procedure shall be executed as the normal method to exchange application data for a user (USR) once the challenge/reply authentication procedure has been successfully completed for the same user.

The following requirements shall be satisfied:

a) This procedure shall be performed for at least each user added (or preconfigured) and owning the update key, whenever a triggering condition in Table 34 occurs. All triggering conditions listed in Table 34 shall be verified for each user added (or preconfigured).

b) This procedure shall be tested at least once for each base protocol ASDU supported by the DUT, in control or monitor direction according to the station type.

7.7.2 Controlling station

7.7.2.1 Normal procedure test cases

Table 34 – Aggressive mode authentication: Controlling station normal procedure tests

No.	Test	Action	Reference	Required
7.7.2.1.1	Station has a Critical ASDU pending to be sent for a USR.	Send S_AR_NA_1 for the same USR encasing the Critical ASDU to be sent.	IEC TS 60870-5-7:2013, 4.5 IEC TS 60870-5-7:2013, 8.2	M
7.7.2.1.2	Reception of a valid S_AR_NA_1	Process the Critical ASDU encased in the S_AR_NA_1 received.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.1.3	Reception of a Non-Critical ASDU	Process the ASDU received.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.1.4	Execution of base protocol procedure	While executing the Aggressive Mode Authentication, the DUT performs the base protocol procedure according to the critical ASDU sent/received as specified in IEC 60870-5-101 / IEC 60870-5-104.	IEC 60870-5-101 IEC 60870-5-104	M

7.7.2.2 Resiliency test tases

Table 35 – Aggressive mode authentication: Controlling station resiliency tests

No.	Test	Action	Reference	Required
7.7.2.2.1	Reception of a Critical ASDU	Discard the ASDU received. Increment the Critical Messages Received statistic. Increment the Discarded Messages statistic.	See NOTE (1)	M
7.7.2.2.2	Reception of a S_AR_NA_1 with USR <> 1 (default)	Discard the ASDU received. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.2.3	Reception of a S_AR_NA_1 while Session Key is NOT VALID (key status <> OK).	Discard the ASDU received. Increment the Unexpected Messages statistic. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.2.4	Reception of a S_AR_NA_1 with a NOT valid MAC	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.2.5		If Transmit Error Messages Option is enabled and if Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5
7.7.2.2.6		If Authentication Failures <= Max Authentication Failures: - Increment the Authentication Failures statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M

No.	Test	Action	Reference	Required
7.7.2.2.7		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys <= Max Authentication Rekeys: - Reset the Authentication Failures statistic - Increment the Authentication Rekeys statistic - Initiate the Session Key Change procedure	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.2.8		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys > Max Authentication Rekeys: - Reset the Authentication Failures statistic - If operating over TCP/IP: Close Connection	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.2.2.9	Reception of an unexpected ASDU (unsolicited or unexpected in this procedure)	Discard the message Increment the Unexpected Messages statistic Increment the Discarded Messages statistic		M
1) This test case is based on pending changes in the referenced technical specification IEC TS 60870-5-7: Aggressive Mode cannot be disabled.				

7.7.3 Controlled station

7.7.3.1 Normal procedure test cases

Table 36 – Aggressive mode authentication: Controlled station normal procedure tests

No.	Test	Action	Reference	Required
7.7.3.1.1	Station has a Critical ASDU awaiting to be sent	Send S_AR_NA_1 encasing the Critical ASDU to be sent.	IEC TS 60870-5-7:2013, 4.5 IEC TS 60870-5-7:2013, 8.2	M
7.7.3.1.2	Reception of a valid S_AR_NA_1 for a USR allowed to perform the function requested by this ASDU in the Controlled Station by RBAC	Process the Critical ASDU encased in the S_AR_NA_1 received.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.1.3	Execution of base protocol procedure	While executing the Aggressive Mode Authentication, the DUT performs the base protocol procedure according to the critical ASDU sent/received as specified in IEC 60870-5-101 / IEC 60870-5-104.	IEC 60870-5-101 IEC 60870-5-104	M

7.7.3.2 Resiliency Test Cases

Table 37 – Aggressive Mode Authentication: Controlled station resiliency tests

No.	Test	Action	Reference	Required
7.7.3.2.1	Expected Session Key Change Timeout expires for a USR	Set Session Key Status to NOT INIT for that USR. Stop sending S_AR_NA_1 for that USR.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.2	Expected Session Key Change Count exceeded for a USR	Set Session Key Status to NOT INIT for that USR. Stop sending S_AR_NA_1 for that USR.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.3	Reception of a Critical ASDU	Increment the Critical Messages Received statistic. Discard the ASDU received. Increment the Discarded Messages statistic.	See NOTE (1)	M
7.7.3.2.4	Reception of a S_AR_NA_1 for a NOT valid USR (not created in the Controlled Station)	Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.5	Reception of a S_AR_NA_1 for a USR while Session Key is NOT VALID (key status <> OK) for that USR.	Increment the Unexpected Messages statistic. Discard the ASDU received. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.6	Reception of a S_AR_NA_1 with a NOT valid MAC.	Discard Critical ASDU pending authentication. Increment the Discarded Messages statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.7		If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 1 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.3.5 Table 30	IEC 60870-5-7 PICS 10.5

No.	Test	Action	Reference	Required
7.7.3.2.8		If Authentication Failures <= Max Authentication Failures: - Increment the Authentication Failure statistic.	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.9		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys <= Max Authentication Rekeys: - Reset the Authentication Failures statistic - Increment the Authentication Rekeys statistic - Set the Session Key Status to AUTH_FAIL	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.10		If Authentication Failures > Max Authentication Failures and if Authentication Rekeys > Max Authentication Rekeys: - Reset the Authentication Failures statistic - If operating over TCP/IP: Close Connection	IEC TS 62351-5:2013, 7.3.3.5 Table 30	M
7.7.3.2.11	Reception of a S_AR_NA_1 for a USR NOT allowed to perform the function requested by this ASDU in the Controlled Station by RBAC.	Increment the Authorization Failures statistic. Discard the ASDU received. Increment the Discarded Messages statistic. If Transmit Error Messages Option is enabled and if the Error Messages Sent <= Max Error Messages: - Send an Error Message with ERR = 7 - Increment the Error Messages Sent statistic	IEC TS 62351-5:2013, 7.3.6.7	IEC 60870-5-7 PICS 10.6 IEC 60870-5-7 PICS 10.5
1) This test case is based on pending changes in the referenced technical specification IEC TS 60870-5-7: Aggressive Mode cannot be disabled.				

8 Tests results chart

8.1 Verification of configuration parameters

Table 38 – Test results chart: Configuration parameters

Configuration parameters		√..... indicates the Test Case has PASSED FAIL..... indicates the Test Case has FAILED N.A..... indicates that Configuration Value is NOT SUPPORTED by the device Empty..... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in the standard	
Test	**No.**	**Description**	**Result**
System Definition	5.2.1	Station Type (Controlling, Controlled)	
	5.2.2	Maximum frame length L (control direction)	
	5.2.3	Maximum frame length L (monitor direction)	
	5.2.4	Number of octets for Cause of Transmission of ASDU	
	5.2.5	Number of octets for Common Address of ASDU	
	5.2.6	Number of octets for Information Object Address	
Application Security Extension	5.3.1	MAC Algorithm (MAL)	
	5.3.2	Key Wrap Algorithm (KWA)	
	5.3.3	Update Key Change method (KCM)	
	5.3.4	User Status Change method	
	5.3.5	Use of Error Messages	
	5.3.6	Configurable Parameters	
	5.3.7	Configurable statistic thresholds and statistic information object addresses	
	5.3.8	Critical functions	

8.2 Verification of communication

8.2.1 ASDUs segmentation control

Table 39 – Test results chart: ASDU segmentation control

Verification of communication **ASDUs segmentation control**	Record the test cases result on the right for each configuration value supported (see Clause 5): √..... indicates the Test Case has PASSED FAIL..... indicates the Test Case has FAILED N.A..... indicates that Configuration Value is NOT SUPPORTED by the device Empty..... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in the standard	**Station Type**	
		Controlling Station	**Controlled Station**
No.	**Description**	**Result**	
6.2.1	Transmission of an ASDU shorter than or equal to the maximum length of the IEC 60870-5 data link or APCI frame		
6.2.2	Transmission of an ASDU longer than the maximum length of the IEC 60870-5 data link or APCI frame		
6.2.3	Reception of a single ASDU segment shorter than or equal to the IEC 60870-5 data link or APCI frame with FIR and FIR bits set		
6.2.4	Reception of a segment with FIR bit set while no segment series is in progress		
6.2.5	Reception of a segment in which TypeID, VSQ, CASDU or COT not matching that in the first segment of the ASDU segment series		
6.2.6	Reception of a segment that is octet-for-octet identical to the preceding segment in the ASDU segment series		
6.2.7	Reception of a segment with the FIR bit set while ASDU segment series is already in progress		
6.2.8	Reception of a segment with the FIR bit cleared and the Sequence Number other than the expected incremental number		

8.2.2 User management ASDUs

Table 40 – Test results chart: User managements ASDUs

Verification of communication **User management ASDUs**		Record the test cases result on the right for each configuration value supported (see Clause 5): √..... indicates the Test Case has PASSED FAIL..... indicates the Test Case has FAILED N.A..... indicates that Configuration Value is NOT SUPPORTED by the device Empty..... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in the standard	**Station Type**	
			Controlling Station	**Controlled Station**
Test	**No.**	**Description**	**Result**	
S_UC_NA_1	6.3.1.1	VSQ: Variable Structure Qualifier		
ASDU 88	6.3.1.2	COT: Cause of Transmission		
User Certificate	6.3.1.3	KCM: Key Change Method		
	6.3.1.4	CDL: Certification Data Length		
	6.3.1.5	CD: Certification Data		
S_US_NA_1	6.3.1.6	VSQ: Variable Structure Qualifier		
ASDU 90	6.3.1.7	COT: Cause of Transmission		
User Status Change	6.3.1.8	KCM: Key Change Method		
	6.3.1.9	OPR: Operation		
	6.3.1.10	SCS: Status Change Sequence Number		
	6.3.1.11	URL: User Role		
	6.3.1.12	UEI: User Role Expiry Interval		
	6.3.1.13	UNL: User Name Length		
	6.3.1.14	UKL: User Public Key Length		
	6.3.1.15	CDL: Certification Data Length		
	6.3.1.16	UN: User Name		
	6.3.1.17	UK: User Public Key		
	6.3.1.18	CD: Certification Data		