



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of IEC TS 62351-100-1:2018.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 96671 2

ICS 33.200

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2018.

Amendments/corrigenda issued since publication

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

TECHNICAL SPECIFICATION



**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

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviated terms	10
3.1 Terms and definitions.....	10
3.2 Abbreviated terms.....	12
4 General	12
4.1 Normatives covered by this technical specification.....	12
4.2 Conformance testing structure	12
4.2.1 General	12
4.2.2 Conformance testing of security extension procedures	13
4.2.3 Conformance testing addressed per station type	14
4.2.4 Normal procedure tests and resiliency tests.....	14
4.3 Conformance testing requirements.....	14
4.3.1 Testing base protocols with security extension.	14
4.3.2 Testing of profiles including TCP/IP	14
4.3.3 Requirements for the device under test	14
4.3.4 Requirements for the test facility	15
4.3.5 Test logging.....	15
5 Verification of configuration parameters.....	16
5.1 General.....	16
5.2 System definition	16
5.3 Application security extension.....	18
6 Verification of Communication	21
6.1 General.....	21
6.2 ASDU segmentation control	21
6.3 Verification of ASDUs	23
6.3.1 User management ASDUs	23
6.3.2 Update key maintenance ASDUs	26
6.3.3 Session key maintenance ASDUs	32
6.3.4 Challenge/reply and aggressive mode authentication ASDUs	35
6.3.5 Security statistics ASDU	39
7 Verification of procedures.....	39
7.1 General.....	39
7.2 User management.....	40
7.2.1 General	40
7.2.2 Controlling station.....	41
7.2.3 Controlled station	43
7.3 Update key maintenance - Symmetric	48
7.3.1 General	48
7.3.2 Controlling station.....	48
7.3.3 Controlled station	52
7.4 Update key maintenance - Asymmetric	54
7.4.1 General	54
7.4.2 Controlling station.....	

7.4.3	Controlled station	59
7.5	Session key maintenance	61
7.5.1	General	61
7.5.2	Controlling station.....	62
7.5.3	Controlled station	67
7.6	Challenge/reply authentication	69
7.6.1	General	69
7.6.2	Controlling station.....	70
7.6.3	Controlled station	76
7.7	Aggressive mode authentication	80
7.7.1	General	80
7.7.2	Controlling station.....	81
7.7.3	Controlled station	84
8	Tests results chart.....	87
8.1	Verification of configuration parameters	87
8.2	Verification of communication	88
8.2.1	ASDUs segmentation control	88
8.2.2	User management ASDUs	89
8.2.3	Update key maintenance ASDUs	90
8.2.4	Session key maintenance ASDUs	92
8.2.5	Challenge/reply and aggressive mode authentication ASDUs	93
8.2.6	Security statistics ASDU	94
8.3	Verification of procedures	95
8.3.1	User management	95
8.3.2	Update key maintenance - Symmetric.....	98
8.3.3	Update key maintenance - Asymmetric	100
8.3.4	Session key maintenance	102
8.3.5	Challenge/reply authentication.....	105
8.3.6	Aggressive mode authentication	109
Figure 1	– IEC TS 62351-5 Security extension procedures	13
Table 1	– Configuration parameters: System definition	17
Table 2	– Configuration parameters: Application security extension	19
Table 3	– ASDU segmentation control.....	22
Table 4	– User management ASDUs.....	23
Table 5	– Update key maintenance ASDUs.....	26
Table 6	– Session key maintenance ASDUs.....	32
Table 7	– Challenge/reply and aggressive mode authentication ASDUs	35
Table 8	– Security statistics ASDU.....	39
Table 9	– User management: Controlling station normal procedure tests	41
Table 10	– User management: Controlling station resiliency tests	42
Table 11	– User management: Controlled station normal procedure tests	43
Table 12	– User management: Controlled station resiliency tests.....	44
Table 13	– Update key maintenance - Symmetric: Controlling station triggering conditions	48

Table 14 – Update key maintenance - Symmetric: Controlling station normal procedure tests	49
Table 15 – Update key maintenance - Symmetric: Controlling station resiliency tests	50
Table 16 – Update key maintenance - Symmetric: Controlled station normal procedure tests	52
Table 17 – Update key maintenance - Symmetric: Controlled station resiliency tests	53
Table 18 – Update key maintenance - Asymmetric: Controlling station triggering conditions	55
Table 19 – Update key maintenance - Asymmetric: Controlling station normal procedure tests	56
Table 20 – Update key maintenance - Asymmetric: Controlling station resiliency tests	57
Table 21 – Update key maintenance - Asymmetric: Controlled station normal procedure tests	59
Table 22 – Update key maintenance - Asymmetric: Controlled station resiliency tests	60
Table 23 – Session key maintenance: Controlling station triggering conditions	62
Table 24 – Session key maintenance: Controlling station normal procedure tests	63
Table 25 – Session key maintenance: Controlling station resiliency tests	64
Table 26 – Session key maintenance: Controlled station invalidating session key	67
Table 27 – Session key maintenance: Controlled station normal procedure tests	68
Table 28 – Session key maintenance: Controlled station resiliency tests	69
Table 29 – Challenge/reply authentication: Controlling station triggering conditions	70
Table 30 – Challenge/reply authentication: Controlling station normal procedure tests	71
Table 31 – Challenge/reply authentication: Controlling station resiliency tests	72
Table 32 – Challenge/reply authentication: Controlled station normal procedure tests	76
Table 33 – Challenge/reply authentication: Controlled station resiliency tests	77
Table 34 – Aggressive mode authentication: Controlling station normal procedure tests	81
Table 35 – Aggressive mode authentication: Controlling station resiliency tests	82
Table 36 – Aggressive mode authentication: Controlled station normal procedure tests	84
Table 37 – Aggressive Mode Authentication: Controlled station resiliency tests	85
Table 38 – Test results chart: Configuration parameters	87
Table 39 – Test results chart: ASDU segmentation control	88
Table 40 – Test results chart: User managements ASDUs	89
Table 41 – Test results chart: Update key maintenance ASDUs	90
Table 42 – Test results chart: Session key maintenance ASDUs	92
Table 43 – Test results chart: Challenge/reply and aggressive mode authentication ASDUs	93
Table 44 – Test results chart: Security statistics ASDU	94
Table 45 – Test results chart: User management procedure – Controlling station	95
Table 46 – Test results chart: User management procedure – Controlled Station	96
Table 47 – Test results chart: Update key maintenance – Symmetric – Controlling station	98
Table 48 – Test results chart: Update key maintenance – Symmetric – Controlled station	99
Table 49 – Test results chart: Update key maintenance – Asymmetric – Controlling station	100

Table 50 – Test results chart: Update key maintenance – Asymmetric – Controlled station	101
Table 51 – Test results chart: Session key maintenance – Controlling station	102
Table 52 – Test results chart: Session key maintenance – Controlled station.....	104
Table 53 – Test results chart: Challenge/reply authentication – Controlling station	105
Table 54 – Test results chart: Challenge/reply authentication – Controlled station	107
Table 55 – Test results chart: Aggressive mode authentication – Controlling station	109
Table 56 – Test results chart: Aggressive mode authentication – Controlled station.....	110

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 60870-5-104-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*

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.

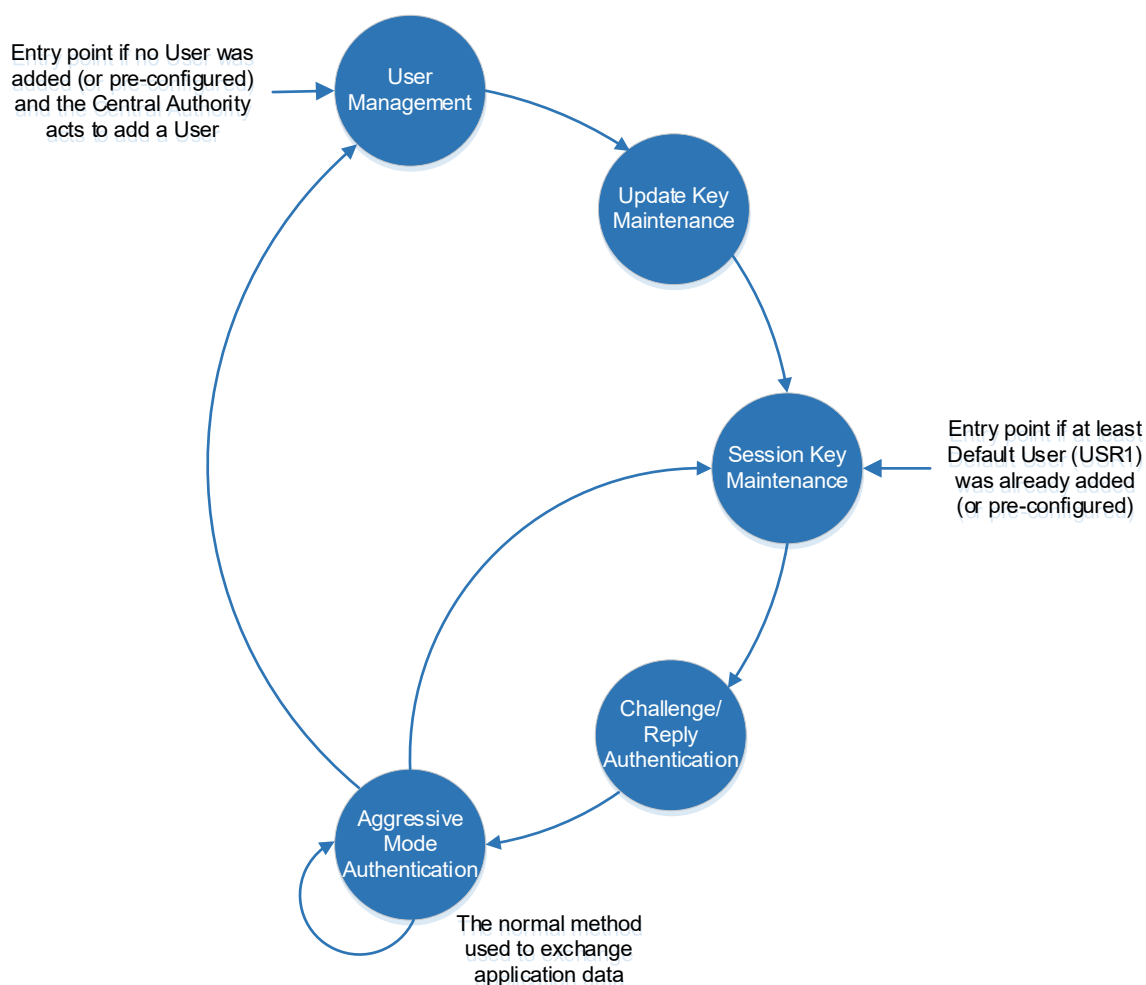
PICS x, x = Mandatory test case if the functionality is enabled in the PICS (by marking the applicable check box), with a reference to the section number of the PICS (x.x).

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.



IEC

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
5.2.2	Frame Length	All conformance tests listed in Clauses 6 and 7 shall be performed at least once for each value of this parameter.		
5.2.3		Maximum length L (control direction)	IEC 60870-5-101:2003, 6.2	M
		Maximum length L (monitor direction)	IEC 60870-5-101:2003, 8.4 IEC 60870-5-104:2006, 9.5	
5.2.4	Cause Of Transmission (COT)	All conformance tests listed in Clauses 6 and 7 shall be performed at least once for each value of these parameters.		
		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 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	IEC 60870-5-101:2003, 7.2.5 IEC 60870-5-101:2003, 8.5 IEC 60870-5-104:2006, 9.5	M

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 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.	IEC TS 62351-5:2013, 8.2.2 IEC TS 60870-5-7:2013, 10.3	M
5.3.2	Key Wrap Algorithm (KWA)	Set of algorithms implemented to encrypt/decrypt the Session Key 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.	IEC TS 62351-5:2013, 8.2.3 IEC TS 60870-5-7:2013, 10.4	M
5.3.3	Update Key Change method (KCM)	Sets of cryptographic algorithms implemented to change the Update Key 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.	IEC TS 62351-5:2013, 8.2.5 IEC TS 60870-5-7:2013, 10.6	M
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. 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.	IEC TS 62351-5:2013, 7.3.3.6 IEC TS 60870-5-7:2013, 10.5	M
5.3.6	Configurable Parameters	Set of the parameters dynamically involved in secure communication. All conformance tests listed in Clauses 6 and 7 shall be performed at least once for one combination of these values.	IEC TS 62351-5:2013, 8.2.5 IEC TS 60870-5-7:2013, 10.8	M
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. All conformance tests listed in Clause 7 shall be performed at least once for one combination of these values.	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
5.3.8	Critical functions	List of functions that are considered critical by the DUT. All conformance tests listed in Clauses 6 and 7 shall be performed at least once for one combination of these values.	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

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 APCl 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 APCl frame.	Station transmit multiple ASDU segments shorter than or equal to the maximum length of an IEC 60870-5 data link or APCl 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 APCl 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 See NOTE (1)	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		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 provided 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