IEC TS 62351-100-4

Edition 1.0 2023-11

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communication security –
Part 100-4: Cybersecurity conformance testing for IEC 62351-4

IEC TS 62351-100-4:2023-11(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC TS 62351-100-4

Edition 1.0 2023-11

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communication security – Part 100-4: Cybersecurity conformance testing for IEC 62351-4

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-7903-8

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 COMMUNICATION SECURITY –

Part 100-4: Cybersecurity conformance testing for 62351-4

FOREWORD

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

IEC TS 62351-100-4 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
57/2505/DTS	57/2564/RVDTS

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

The language used for the development of this Technical Specification is English.

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.

In this document the following print types are used:

- Abstract Syntax Notation One (ASN.1) and W3C XML Schema Definition (W3C XSD) notions are presented in **`bold Courier New`** typeface; and
- when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in **`bold Courier New`** typeface.

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

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

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

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

INTRODUCTION

The quality system of a device producer forms the basis of reliable testing in development and production activities. Many internal tests during the development of a device result in a unit level test performed at least by the provider and – if required by applicable standards – by an independent test authority. In the context of this document, the term type test is restricted to the functional behavior of the device.

To validate the results of some tests, internal IED information should be made available (see 5.3.4). These requirements are beyond those specified in IEC 62351-4 and therefore the manufacturer/vendor shall describe in Table 2 how the IED can expose the required information.

Conformance testing does not replace project-specific system-related tests such as the POC (Proof Of Concept) FAT (Factory acceptance Test) and SAT (Site Acceptance Test). The POC, FAT and SAT are based on specific customer requirements for a dedicated substation automation system and are done by the system integrator and normally witnessed by the customer. These tests increase the confidence level that all potential problems in the system have been identified and solved. These tests establish that the delivered substation automation system is performing as specified. The conformance testing reduces the risks of failure during the POC, FAT and SAT.

The purpose of this part of IEC 62351 is to cover all possible situations taking into consideration the normal operating test cases and the resiliency test cases to demonstrate the capability of the DUT to operate with other devices in the specified way according to IEC 62351-4:2018/AMD1:2020, and also according to the PID (Protocol Implementation Document). Testing of Application layer protocol (61860-8-1, 61850-8-2 or ICCP) features or performances is out of scope.

Through this part of IEC 62351, a test facility can prove that the DUT communication subsystem (or a part of it) conforms to IEC 62351-4:2018/AMD1:2020.

The test cases described in this specification do not guarantee full cybersecurity conformance testing. It is to be complemented with other test suites.

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

Part 100-4: Cybersecurity conformance testing for 62351-4

1 Scope

This part of IEC 62351, which is a technical specification, describes test procedures for interoperability conformance testing of data and communication security for power system automation and protection systems which implement MMS, IEC 61850-8-1 (MMS), IEC 61850-8-2 (XMPP) or any other protocol implementing IEC 62351-4:2018/AMD1:2020. The tests described in this document cover only E2E security testing and do not evaluate A-security[1] profile implementation. Thus, citing conformance to this document does not imply that any particular security level has been achieved by the corresponding product or by the system in which it is used.

The goal of this document is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. It is expected that using this document during testing will minimize the risk of non-interoperability. Additional testing and assurance measures will be required to verify that a particular implementation of IEC 62351-4:2018/AMD1:2020 has correctly implemented all the security functions and that they can be assured to be present in the delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify available common procedures and definitions for conformance and/or interoperability testing of IEC 62351-4:2018/AMD1:2020.

This document deals mainly with cyber 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.

T-profile testing is to be performed prior to E2E security profile testing. T-profile testing is described in IEC 62351-100-3 in the context of IEC 61850-8-1. T-profile testing for IEC 61850-8-2 is to be described in the corresponding IEC 61850-8-2 test specification.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62351-4:2018, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*
IEC 62351-4:2018/AMD1:2020

IEC 62351-3:2023, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

---

[1] A-profile is specified in IEC 62351-4:2020 for backward compatibility with IEC 62351-4:2007.

IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the PID Protocol Implementation Document and the following apply.

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

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

3.1.1
application context
set of rules shared in common by two application-entity in order to support an association (in an OSI operational environment)

[SOURCE: IEC 62351-4:2018/AMD1:2020, 3.1.5]

3.1.2
application entity
active element embodying a set of capabilities which is pertinent to communication systems, and which is defined for the application layer

[SOURCE: IEC 62351-4:2018/AMD1:2020, 3.1.6]

3.1.3
association
cooperative relationship between application-entity invocations, which enables the communication of information and the coordination of their joint operation for an instance of communication

[SOURCE: Rec. ITU-T X.217 (1995), 3.5.1]

3.1.4
E2E security
security facilities at the application layer that ensures data origin authentication and integrity end-to-end with or without confidentiality (encryption) between two entities with zero or more intermediate entities

[SOURCE: IEC 62351-4:2018/AMD1:2020, 3.1.18]

3.1.5
environment protocol data unit
application protocol data unit (APDU) that is carrying protocol control information for the environment protocol in addition to carrying a security protocol data unit

[SOURCE: IEC 62351-4:2018/AMD1:2020, 3.1.20]

3.1.6
protected protocol data unit
application protocol data unit (APDU) defined by a protected application protocol

[SOURCE: IEC 62351-4:2018/AMD1:2020, 3.1.28]

3.1.7
protocol control information
information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation

3.1.8
Protocol Implementation Document (PID)
document which includes all the required parameters, settings and options for a particular protocol implemented in the IED

Note 1 to entry: This document will include the PICS and PIXIT that will be implemented during the tests.

3.2 Abbreviated terms

AA	Application Association
TP	Two-Party
AEAD	Authenticated Encryption with Associated Data
DUT	Device Under Test
TEQ	Test Equipment
PCI	Protocol Control Information
PDU	Protocol Data Unit
APDU	Application PDU
EnvPDU	Environment PDU
PrPDU	Protected PDU
SecPDU	Secured PDU
SAOC	Send Application Object Classes
RAOC	Receive Application Object Classes
PID	Protocol Implementation Document that includes PICS and PIXIT
N/R	Note required

4 Application structure and information flow

4.1 Overview

This clause describes the application structure and information flow specified by IEC 62351-4:2018/AMD1:2020. These structures will be used in this document to specify the configuration parameters and describe the test procedures.

4.2 Application entity structure

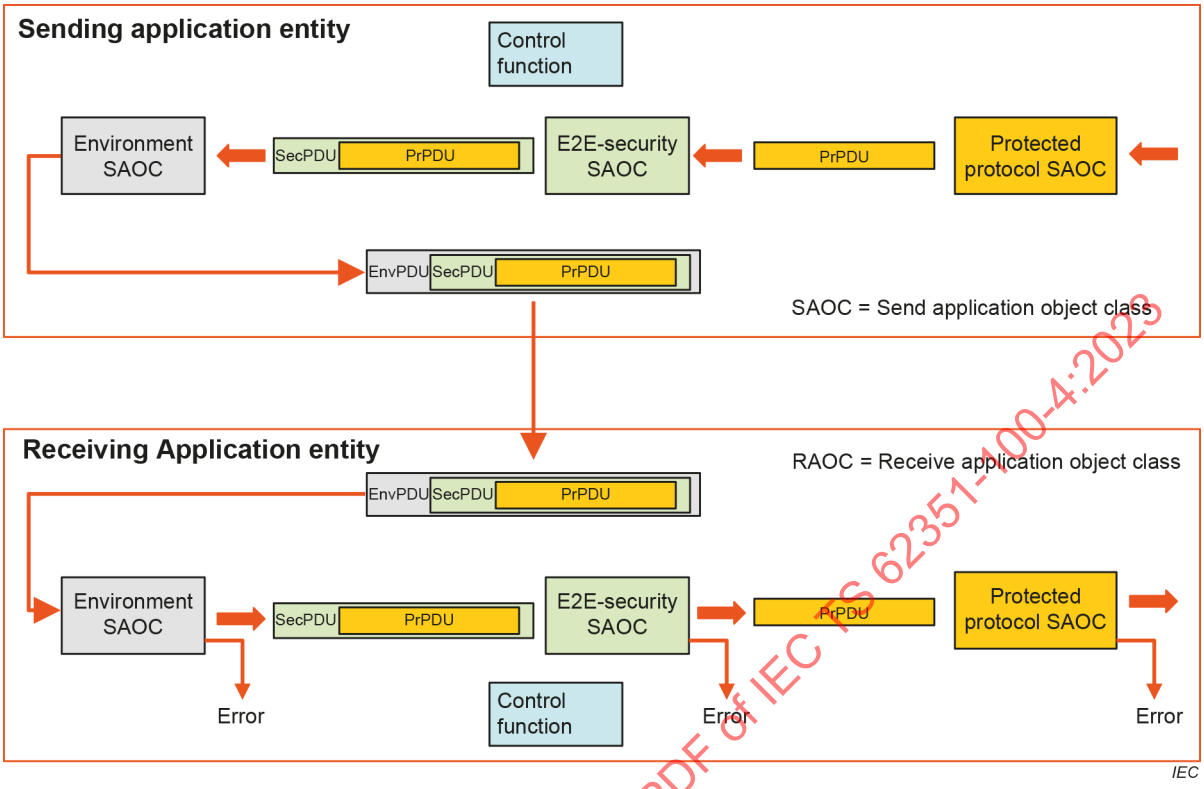

Figure 1 – Application entity structure and information flow

Figure 1 illustrates the proposed structure of application entity components, their inner relationship, and the information flow. The figure is not intended to reflect a possible implementation structure but is used to reflect the relationship between the different components of an application entity.

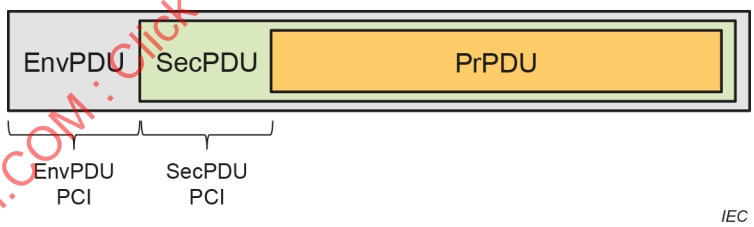

Figure 2 – Relationships between APDUs

Figure 2 illustrates the relationship between APDUs as reflected by the model shown in Figure 1. An APDU of a protected protocol is called a protected PDU (PrPDU). An APDU of the E2E security is called a security PDU (SecPDU). It holds security protocol control information and may hold a PrPDU. The APDU transporting a SecPDU is called the Environment PDU (EnvPDU). In addition to the holding the SecPDU, it holds protocol control information necessary for the overall operation for the environmental handling. An APDU consists of a header and, if relevant, of a payload. The header holds the protocol control information (PCI) controlling the underlying protocol. For an EnvPDU, a SecPDU is the payload, while a PrPDU is the payload for a SecPDU.

As illustrated in Figure 1, an application entity in the context of this document consists of SAOCs and RAOCs. The control function included in the figure provides the overall coordination of the application entity. The implementation of control function may reflect the overall application that includes the capabilities of the enclosing SAOCs and RAOCs.

Object classes defined in this way have subclasses for specific purposes. As an example, the E2E-security SAOC has a subclass for each type of SecPDU to be generated. Each such subclass is described in term of required input and generated output.

Clause 9 describes the SecPDU subclasses specified in IEC 62351-4:2018/AMD1:2020.

Clause 10 describes the EnvPDU subclasses for MMS implementation (IEC 61850-8-1 or ICCP) specified in 62351-4:2018/AMD1:2020.

Clause 11 describes the EnvPDU subclasses for XMPP implementation (IEC 61850-8-2) specified in IEC 62351-4:2018/AMD1:2020.

4.3 Relationship to test structure

The test structure and test methodology may also be illustrated using Figure 1. Consider the top part of Figure 1 (the sending application entity) as the device under test (DUT) and the lower part (the receiving application entity) as the testing equipment (TEQ).

The DUT is made to send EnvPDUs, which are then analyzed by the TEQ. The DUT may be triggered to send EnvPDUs in two ways:

a) The DUT is by external stimuli instructed to issue particular types of EnvPDUs.
b) The TEQ sends EnvPDUs to the DUT, which requires the DUT to respond with corresponding EnvPDUs.

The tests consist of:

a) Test procedures specified for both the OSI environment and the XMPP environments (Clauses 6 and 7) and are applied depending on which environment, the DUT claims conformance. These tests validate at the same time the EnvPDU and the SecPDU behaviour of the DUT. PCI items (EnvPDU and SECPDU components) are listed in the subclasses (Clauses 9, 10 and 11) with required content specified and against which the DUT emitted EnvPDUs and SecPDUs are checked. Clauses 6 and 7 also describe tests sequence to validate the required handshaking between the DUT and the TEQ.
b) Resiliency tests to validate the capability of the DUT to recover from errors in the implemented protocol. For these tests, the TEQ sends PDU that contains error. Clauses 6 and 7 describe contingency tests resulting from EnvPDU errors and Clause 8 from SecPDU errors. Clause 8 tests are independent on the operational environment.

The document is structured as depicted in Figure 3.

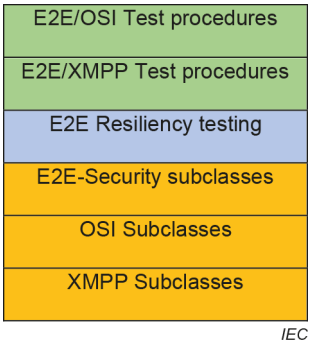

Figure 3 – Structure for test specifications

5 General

5.1 General guidelines

The test environment should be as close as possible to the final environment. To perform the test, a specially designed testing device (TEQ) is used to test the device under test (DUT). Since the IED can be tested in server or client mode, two TEQs exist.

To realize the tests described in this standard, a TEQ compliant to IEC 62351-4:2018/AMD1:2020 shall be used. The TEQ shall offer the capability of analysis all the IEC 62351-4:2018/AMD1:2020 requirements and be able to generate an invalid message to test the robustness of the device under test (DUT). The DUT should provide mechanisms to permit the validation of the results of the tests and give the secure connection status. Table 2 describes means of reporting/displaying internal status to provide to the test engineer enough information in order to validate the results of the tests.

The test facility will likely use a single server/client simulator, but there is no restriction on using one server/client which only supports certain communication services and using another to do the rest, i.e. as long as the server(s)/client(s) simulators can cover the input requirements to the test case/DUT. Such test environment adaptions should be documented in the test report.

5.2 Test methodology

5.2.1 General

The tests are realized in a non-intrusive mode. The device under test (DUT) has the same software and parameters as the production system. In order to realize the conformity testing, IED functions, at application level (IEC 61850-8-1, IEC 61850-8-2 or ICCP), are used to establish a secure connection. When an operation fails, the use of cybersecurity logs will allow the identification of the failing tests. The tests are grouped in a table for each type of tests. In these tables, the test procedures have numeric references. If the test case needs more than one step, it will be enumerated as 1a), 1b) … The test cases in this document should be referred as in the following example: Table 1-1a).

The detailed test procedures are not part of this document and are left to the conformance test body. Test labs claiming the ability to perform conformance testing to these parts of IEC 62351 shall be accredited for quality and technical competency by an internationally recognized organization.

5.2.2 Normal procedure tests and resiliency tests

IEC 62351-4:2018/AMD1:2020 specifies how each IED (client and server) shall execute the procedures in normal conditions (expected behaviour) and also how it shall behave when unexpected or fault events occur during their execution (negative behaviours). The tests cases are thus divided in two categories: the normal procedure 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 AT LEAST ONCE for one mandatory cryptographic algorithms required by the standard referencing IEC 62351-4:2018/AMD1:2020, with the mandatory key length required by IEC 62351-4:2018/AMD1:2020. PICS Table 11 – Conformance to cryptographic algorithms for E2E-security in IEC 62351-4:2018/AMD1:2020 lists the cipher suites supported by the DUT and those selected for the tests.

5.2.3 SubClass descriptions

Clauses 9, 10 and 11 define the different subclasses used for E2E security.

The core definition for E2E (SecPDU) is defined in Clause 9 while Clauses 10 and 11 define subclass used for OSI and XMPP EnvPDU.

The tables in these clauses define the expected value of the different data components. The tests refer to these tables in order to help the test engineer in interpreting the test results.

5.3 Conformance testing requirements

5.3.1 Testing within the context of an application

The test cases listed in this document shall be executed within the context of an application. The DUT claiming conformance to IEC 62351-4:2018/AMD1:2020 shall execute an application protocol defined in a standard requiring conformance to the IEC 62351-4:2018/AMD1:2020.

5.3.2 Requirements for the device under test

Before the beginning of the testing, the Protocol Implementation Document (PID) that includes all the required parameters, settings and options for a particular protocol implemented in the IED shall be prepared. This document will include the PICS and PIXIT that will be implemented during the tests.

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

a) The DUT ready for testing;

b) Protocol Implementation Conformance Statement (PICS);

c) Protocol Implementation eXtra Information for Testing (PIXIT)

d) 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 are satisfied:

e) The DUT is able to operate as a client or server station according to the PID (depending on the type of DUT).

f) The DUT must be fully configured according to the supported features declared in the PICS. Testing can then be executed to all the functionality of the protocol implementation as described in the test cases.

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

h) Verification of the data points shall be possible in a human readable way or format, and the verification of analog and digital status changes is possible. Such verification is recommended to be defined in the PIXIT.

i) The DUT has successfully passed the readiness requirements like PICS and PIXIT containing all required information and DUT is configured to prove all supported functionality.

IEC 61850 DUT shall also include:

j) IED capability description (ICD) or Instantiated IED description file (IID) as supported (in SCL format)

5.3.3 Requirements for the test facility

The following requirements shall be satisfied by the test facility:

The documentation provided with the DUT shall be inspected for correctness and completeness. Also, the software and hardware versions of the DUT shall be verified.

- 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 Table 3 or Table 4 shall be performed with no errors detected during testing.
- The test cases may require many steps that should be performed in the order listed in the table.
- For each test case, the test results need to be marked in the appropriate column of the test result chart. Each test case can either pass the test (Passed), fail the test (Failed), or the test case was not performed (Reason why the test is not performed).
- Release a conformance test report of the DUT to the test initiator.

The tests can be verified automatically by a testing software or verified manually by review of the test history log after execution of the test procedures. The TEQ is preferably flexible in adding or changing test cases to be adaptable to changes in the protocol standard and the PID provided with the DUT. In all cases, the test shall be reproducible.

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.

For client testing, a homologated server must be used. This server must have the capability of sending conformant and erroneous message.

For server testing, a homologated client must be used. This client must have the capability of sending conformant and erroneous message.

Conformity tests apply only to a specific software and hardware version.

5.3.4 Test Validation

During the execution of conformance testing, the following information should be made available by the DUT for test results analysis:

- Communication events (association establishment, rekey (for E2E security), association release, data transfer);
- Certificate check results (e.g., valid, expired, revoked, invalid key length, invalid signature);
- Change cipher result (e.g., unsupported).
- The security events raised by the DUT (required by IEC 62351-4:2018/AMD1:2020) whenever a negative behaviour occurs while performing resiliency tests.

Table 2 shall be filled by the manufacturer to indicate how the information is made available to the test engineer.

5.4 PICS

The test procedures described in this document are at an abstract level. The conformity body should develop detailed test procedures to perform conformity testing. To do so, the manufacturer must prepare the PICS for the application-level implementation. The tests requirements described in this document can be applied to IEC 61850-8-1, IEC 61850-8-2 and ICCP. All these protocols shall support PrPDU defined in IEC 62351-4:2018/AMD1:2020. Moreover, IEC 62351-4:2020 specifies how to implement EnvPDU within an OSI environment and XMPP environment. IEC 62351-6:2020 includes PICS for IEC 61850-8-1 ISO 9506 profile security.

5.5 PIXIT

This document specifies PIXIT to indicate how to conduct and document the test procedures. Table 1 defines the base profile and Table 2 lists general PIXIT that cover all the tests. The manufacturer must prepare the PIXIT for the implementation.

Table 1 – PIXIT for Base Profile

ID	Description	Value/Product Behaviour
1	Describe the DUT and architecture configuration used during the tests including but not limited to: • interface for connectivity = Single/Dual (delete as required) • other interface required e.g. monitoring available via DUT webserver • Primary Time Source (e.g. NTP , PTP) • Security Features available (e.g. logging &/or Syslog enabled, port enabled, Authentication enabled) Y/N (delete as required) • Describe how DUT Publishes Errors? • Describe how DUT Records Errors? Certificate Authority: • ALL mandatory CIPHERS supported • Enrolment method used e.g. EST • Certificate Expiry 1hr/24hr/Other	
2	Please describe the method(s) by which the DUT is forced from its base profile to security enabled, e.g. Configuration Tool, HMI etc.?	

Table 2 – PIXIT for Secure Communication

ID	Description	Value/Product Behaviour
1	Generate manually and/or automated and provision a trust anchor key-pair, an intermediate CA key-pair and an entity key-pair as typically a public key certificate with a correspondent private key.	
2	Describe how the DUT exposes the certificate validation results including the components defined in 62351-9	
3	Describe the method(s) by which the DUT is forced to initiate an association Request?	
5	Describe the method(s) by which the DUT exposes an Association Accept?	
6	Describe the method(s) by which the DUT exposes the public-key certificate validation results? How can this information be validated? • DUT records errors • DUT publish errors	
7	Describe the method(s) by which the DUT is forced to initiate Data Transfer	
9	Describe the method(s) by which the DUT validates the 10 minutes difference from the UTC time How can this information be validated? • DUT records errors • DUT publish errors	
10	Describe the method(s) by which the DUT validates ~~time~~ value is received twice within a time span of 10 min? How can this information be validated? • DUT records errors • DUT publish errors	
11	Describe the method(s) by which the DUT validates the signature component? How can this information be validated? • DUT records errors • DUT publish errors	
12	Describe the method(s) by which the DUT handles a P-Abort? How can this information be validated? • DUT records errors • DUT publish errors • Other (please specify)	
13	Describe the method(s) by which the DUT is forced to initiate Data Transfer	

5.6 Tests cases

Table 3 and Table 4 describe the conformity tests for the end-to-end secure mode for the different protected protocols. Two different sets of tests are required since IEC 62351-4:2018/AMD1:2020 specifies different EnvPDU requirements for OSI (IEC 61850-8-1 and ICCP) and XMPP (IEC 61850-8-2) profiles.

Table 3 – IEC 62351-4:2018/AMD1:2020 E2E Compliancy Testing (IEC 61850-8-1 and ICCP)

Test Case ID	Test Case	Description	Results
Table 14	Association establishment Client only	Validate that the DUT initiates properly a secure connection with the server. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 15	Association establishment Server only	Validate that the DUT accepts properly a secure connection from the client. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 16 Table 49	Association establishment – Resiliency tests Client only	Validate the DUT (client) can recover from various errors such as invalid keys, errors in encryption, etc. Table 16 describes the resiliency tests for the EnvPDU. Table 49 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 17 Table 50	Association establishment – Resiliency tests Server only	Validate the DUT (server) can recover from various errors such as invalid keys, errors in encryption, etc. Table 17 describes the resiliency tests for the EnvPDU. Table 50 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 18	Clear data transfer	Validate that the DUT complies to clear data transfer. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 19 Table 52	Clear data transfer - Resiliency tests Client only	Validate the DUT (client) can recover from various errors such as invalid keys, errors in encryption, etc. Table 19 describes the resiliency tests for the EnvPDU. Table 52 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 20 Table 51	Clear data transfer - Resiliency tests Server only	Validate the DUT (server) can recover from various errors such as invalid keys, errors in encryption, etc. Table 20 describes the resiliency tests for the EnvPDU. Table 51 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 21	Encrypted data transfer	Validate that the DUT complies to encrypted data transfer. These tests cover EnvPDU and SecPDU	Optional ☐ Passed ☐ Failed

Test Case ID	Test Case	Description	Results
Table 22 Table 53	Encrypted data transfer – Resiliency tests Client only	Validate the DUT can recover from various errors such as invalid keys, errors in encryption, etc. Table 22 describes the resiliency tests for the EnvPDU. Table 53 describes the resiliency tests for the SecPDU	Optional ☐ Passed ☐ Failed
Table 23 Table 54	Encrypted data transfer – Resiliency tests Server only	Validate the DUT can recover from various errors such as invalid keys, errors in encryption, etc. Table 23 describes the resiliency tests for the EnvPDU. Table 54 describes the resiliency tests for the SecPDU	Optional ☐ Passed ☐ Failed
Table 14	Association release Client only	Validate that the DUT (client) proceeds properly to the disconnection process. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 15	Association release Server only	Validate that the DUT (server) responds properly to the disconnection process. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 24	Rekey initiated by the client	Validate that the DUT (client) successfully updates the keys These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 25	Rekey initiated by the server	Validate that the DUT (server) successfully requires key updates from the client These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed

Table 4 – IEC 62351-4:2018/AMD1:2020 E2E Compliancy Testing (IEC 61850-8-2)

Test Case ID	Test Case	Description	Results
Table 37	Association establishment Client only	Validate that the DUT initiates properly a secure connection with the server. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 38	Association establishment Server only	Validate that the DUT accepts properly a secure connection from the client. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 39 Table 49	Association establishment – Resiliency tests Client only	Validate the DUT (client) can recover from various errors such as invalid keys, errors in encryption, etc. Table 39 describes the resiliency tests for the EnvPDU. Table 49 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 40 Table 50	Association establishment – Resiliency tests Server only	Validate the DUT (server) can recover from various errors such as invalid keys, errors in encryption, etc. Table 40 describes the resiliency tests for the EnvPDU. Table 50 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 41	Clear data transfer	Validate that the DUT complies to clear data transfer. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 43 Table 52	Clear data transfer - Resiliency tests Client only	Validate the DUT (client) can recover from various errors such as invalid keys, errors in encryption, etc. Table 43 describes the resiliency tests for the EnvPDU. Table 52 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 42 Table 51	Clear data transfer - Resiliency tests Server only	Validate the DUT (server) can recover from various errors such as invalid keys, errors in encryption, etc. Table 42 describes the resiliency tests for the EnvPDU. Table 51 describes the resiliency tests for the SecPDU	mandatory ☐ Passed ☐ Failed
Table 44	Encrypted data transfer	Validate that the DUT complies to encrypted data transfer. These tests cover EnvPDU and SecPDU	Optional ☐ Passed ☐ Failed

Test Case ID	Test Case	Description	Results
Table 45 Table 53	Encrypted data transfer – Resiliency tests Client only	Validate the DUT can recover from various errors such as invalid keys, errors in encryption, etc. Table 22 describes the resiliency tests for the EnvPDU. Table 53 describes the resiliency tests for the SecPDU	Optional ☐ Passed ☐ Failed
Table 46 Table 54	Encrypted data transfer – Resiliency tests Server only	Validate the DUT can recover from various errors such as invalid keys, errors in encryption, etc. Table 45 describes the resiliency tests for the EnvPDU. Table 54 describes the resiliency tests for the SecPDU	Optional ☐ Passed ☐ Failed
Table 37	Association release Client only	Validate that the DUT (client) proceeds properly to the disconnection process. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 38	Association release – server	Validate that the DUT (server) responds properly to the disconnection process. These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 47	Rekey initiated by the client	Validate that the DUT (client) successfully updates the keys These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed
Table 48	Rekey initiated by the server	Validate that the DUT (server) successfully requires key updates from the client These tests cover EnvPDU and SecPDU	mandatory ☐ Passed ☐ Failed

6 E2E conformity testing in an OSI environment

6.1 Conformance tables for E2E OSI-security profile

The following conformance tables (Table 6, Table 7, Table 8, Table 9, Table 10, Table 11, Table 12 and Table 13) are used to provide an overview and details about the IEC 61850 <Client and/or Server> product identified as <device ID and name>, with firmware <version>.

The statement shall identify the applicable details required for each of the Test Cases defined in IEC 62351-100-4 that are either:

m: Mandatory support. The item shall be implemented.

c: Conditional support. The item shall be implemented as specified by the condition.

o: Optional support. The item may be, but need not be implemented.

i: Out of scope

Table 5 – Base Profile – E2E Security

		Client	Server	Comments
Base Profiles				
5-1	Server IEC 61850-8-1 Compliant	N/A		
5-2	Client IEC 61850-8-1 Compliant		N/A	
5-3	Server ICCP Compliant	N/A		
5-4	Client ICCP Compliant		N/A	
5-5	Server IEC 62351-3:2014/AMD2:2020 Requirement Support	N/A		IEC 62351-6 PICS
5-6	Client IEC 62351-3:2014/AMD2:2020 Requirement Support		N/A	IEC 62351-6 PICS

Table 6 – Protocol Handshake – E2E Security

	Services	AA: TP	Client (C)	Server (S)	Comments
IEC 61850 Application association					
6-1	Association Conformance Block Supported	TP			When supported completion of Table 7-1 to Table 7-3 is required to state support or non-support

Table 7 – IEC 61850 Application Association – E2E Security

	Services	AA: TP	Client (C)	Server (S)	Comments
IEC 61850 Application association					
7-1	Associate	TP			
7-2	Abort Processing	TP	C1	C1	
7-3	Release Processing	TP	C1	C1	
C1: At least Abort or Release shall be supported (see IEC 62351-4)					

Table 8 – OSI EnvPDU Supported – E2E Security

	Services	AA: TP	Client (C)	Server (S)	Comments
OSI EnvPDU Supported					
8-1	OSI EnvPDU Supported according to IEC 62351-4:2018/AMD1:2020	TP			When supported completion of Table 9.2-Table 9.7 is required to state support or non-support

Table 9 – OSI EnvPDU Subclass Supported – E2E Security

	Services	AA: TP	Client (C)	Server (S)	Comments
OSI EnvPDU Subclass Supported					
9-1	OSI Association Request	TP			

9-2	OSI Association Response	TP			
9-3	OSI Abort	TP			
9-4	OSI Release Request	TP			
9-5	OSI Release Response	TP			
9-6	OSI Clear Data Transfer	TP			
9-7	OSI Encrypted Data Transfer	TP			

Table 10 – E2E SecPDU Subclass Supported

	Services	AA: TP	Client (C)	Server (S)	Comments
OSI SecPDU Subclass Supported					
10-1	`HandshakeReq`	TP			
10-2	`HandshakeACC`	TP			
10-3	`ApplicationReject`	TP			
10-4	`HandshakeSecReject`	TP			
10-5	`ReleaseReq`	TP			
10-6	`ReleaseRsp`	TP			
10-7	`ClearTransfer`	TP			
10-8	`EncrTransfer`	TP			
10-9	`HandshakeSecAbort`	TP			
10-10	`DtSecAbort`	TP			
10-11	`ApplAbort`	TP			

To be specified by referencing specification. At least one row shall specify "m" for both client and server.

Table 11 – OSI Mode of encryption – E2E Security

	Services	AA: TP	Client (C)	Server (S)	Comments
Mode of encryption					
11-1	Use of authenticated encryption (AE)	TP			Use of single algorithm for encryption and integrity
11-2	Non-use AE	TP			Non-use of encryption or separate algorithms for encryption and integrity

Table 12 – Cryptographic algorithms – E2E Security

	Services		AA: TP	Client (C)	Server (S)	Comments
Public-key algorithms						
12-1	rsaEncryptionAlgorithm		TP			Mandatory
12-2	ecPublicKey	secp256r1	TP			Mandatory
		brainpoolP256r1	TP			Mandatory
Signature algorithms						
12-3	`sha256WithRSAEncryptionAlgorithm`		TP			Mandatory

12-4	ecdsa-with-SHA256-Algorithm	TP			Mandatory
Symmetric encryption algorithms					
12-5	aes128-CBC	TP			C1
12-6	aes256-CBC	TP			C1
Authenticated encryption algorithms					
12-7	aes128- GCM	TP			C2
12-8	aes256- GCM	TP			C2
Integrity check value algorithms					
12-9	hmacWithSHA256	TP			C3
12-10	aes128-GCM	TP			C3
12-11	aes256-GCM	TP			C3

C1: Shall be "m" if E2E security with encryption is declared and non-use of authenticated encryption is declared. Otherwise, it shall be "i".

C2: Shall be "m" if E2E security with encryption is declared and use of authenticated encryption is declared. Otherwise, it shall be "i".

C3: Shall be "m" if non-use of authenticated encryption is declared (see Table 11). Otherwise, it shall be "i".

Table 13 – ASN.1 Objects – E2E Security

	Ed.	Services	AA: TP	Client (C)	Server (S)	Comments
ASN-1 Authentication Object Identifier						
13-1	2	`E2E-Security {iso(1) standard(0) iec62351(62351) part4(4) modules(0) e2e-security(1) version1(1)}`	TP			IEC-62351-4:2018/AMD1:2020

6.2 E2E Test Procedures for OSI environment

6.2.1 Association Management

The test procedure describes how to validate the initial connection between a client and a server.

The normal result of this test procedure is a successful connection without any exception.

The tester will need to define the high-level test procedure that will initiate the handshake process.

During the following tests, the testers will be able to diagnose using the approach described in Table 2.

Table 14 – Verification of Client handshake request procedure in OSI environment

No	Test	Expected result	Reference	Required
1	Make the DUT to initiate an association. 1) EnvPDU: see Table 68 2) SecPDU: see Table 55	TEQ shall validate the received PDU. 1) If the PDU does not contain error, a) TEQ sends the PDU association confirmation: i) EnvPDU: see Table 69 ii) SecPDU: see Table 56 b) The DUT shall indicate successful connection 2) If the PDU contains error, association establishment test fails.	IEC 62351-4:2018/AMD1:2020, 15.3.2 IEC 62351-4:2018/AMD1:2020, 15.3.3 IEC 62351-4:2018/AMD1:2020, 13.1.3 IEC 62351-4:2018/AMD1:2020, 13.1.4 IEC 62351-4:2018/AMD1:2020, 13.3.1.1 PIXIT Table 2	m
2	DUT to release the association issuing **`ReleaseReq`** 1) EnvPDU: see Table 74 2) SecPDU: see Table 66	TEQ shall valid the received PDU. 1) If the PDU does not contain error, a) TEQ sends the PDU release response i) EnvPDU see Table 75 ii) SecPDU: see Table 67 b) The DUT shall indicate connection release 2) If the PDU contains error, association release test fails	IEC 62351-4:2018/AMD1:2020, 15.3.5 IEC 62351-4:2018/AMD1:2020, 15.3.6 IEC 62351-4:2018/AMD1:2020, 13.1.10 IEC 62351-4:2018/AMD1:2020, 13.1.11 IEC 62351-4:2018/AMD1:2020, 13.3.3 PIXIT Table 2	m

Table 15 – Verification of Server handshake request procedure in OSI environment

No	Test	Expected result	Reference	Required
1	Make the TEQ to initiate an association. 1) EnvPDU: see Table 68 2) SecPDU: see Table 55	DUT shall validate the received PDU. 1) If the PDU does not contain error, a) DUT shall send association confirmation: i) EnvPDU see Table 69 ii) SecPDU: see Table 56 b) TEQ shall validate and indicate the received association confirmation 2) If the PDU contains error, the association establishment test fails	IEC 62351-4:2018/AMD1:2020, 15.3.2 IEC 62351-4:2018/AMD1:2020, 15.3.3 IEC 62351-4:2018/AMD1:2020, 13.1.3 IEC 62351-4:2018/AMD1:2020, 13.1.4 IEC 62351-4:2018/AMD1:2020, 13.3.3 PIXIT Table 2	m
2	TEQ to release the association issuing **`ReleaseReq`** 1) EnvPDU: see Table 74 2) SecPDU: see Table 66	DUT shall valid the received PDU. 1) If the PDU does not contain error, a) DUT sends release response i) EnvPDU see Table 75 ii) SecPDU: see Table 67 b) TEQ shall validate and indicate the received release response. 2) If the PDU contains error, the association release test fails	IEC 62351-4:2018/AMD1:2020, 15.3.5 IEC 62351-4:2018/AMD1:2020, 15.3.6 IEC 62351-4:2018/AMD1:2020, 13.1.10 IEC 62351-4:2018/AMD1:2020, 13.1.11 IEC 62351-4:2018/AMD1:2020, 13.3.3 PIXIT Table 2	m

Table 16 describes the tests to verify how the DUT (client) reacts to error conditions. This table includes the tests to be done at the environment level. Tests for secure environment are defined in Table 49.

Table 16 – Handshake request resiliency procedure in OSI environment – Client

No	Test	Expected result	Reference	Required
1	After having received a valid **AARQ-apdu** from the DUT, the TEQ shall send an **AARE-apdu**, with the **indirect-reference** absent.	The DUT shall return an **ABRT-apdu** holding an **OSI-AssoAbr** data value taking the **osiDiag** alternative with the **value protocol-error** to be checked as specified in Table 70	Rec. ITU-T X.227, 9.1, IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1 IEC 62351-4:2018/AMD1:2020, 15.3.4 IEC 62351-4:2018/AMD1:2020, 15.6 PIXIT Table 2	m
2	After having received a valid **AARQ-apdu** from the DUT, the TEQ shall send an **AARE-apdu** with the **result** component set to **accepted** and with and invalid **indirect-reference**.	The DUT shall return an **ABRT-apdu** holding an **OSI-AssoAbr** data value taking the **osiDiag** alternative with the **value invalid-indirect-reference** to be checked as specified in Table 70.	Rec. ITU-T X.227, 9.1, IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1 IEC 62351-4:2018/AMD1:2020, 15.3.4 IEC 62351-4:2018/AMD1:2020, 15.6 PIXIT Table 2	m
3	Continue with the tests described in Table 49			

Table 17 describes the tests to verify how the DUT (server) reacts to error conditions. This table includes the tests to be done at the environment level. Tests for secure environment are defined in Table 50.

Table 17 – Handshake request resiliency procedure in OSI environment – Server

No	Test	Expected result	Reference	Required
1	TEQ to send the DUT an **AARQ-apdu** with a wrong application context.	The DUT shall return an **AARE-apdu** with a) **result** component set to **rejected-permanent**; b) the **result-source-diagnostics** taking the **acse-service-user** alternative with the value **application-context-name-not-supported.**	ITU-T X.227, 9.1 IEC 62351-4:2018/AMD1:2020, 15.3.3	m
2	TEQ to send the DUT an **AARQ-apdu with a wrong indirect-reference in the OSI-AssoReq data value**	The DUT shall return an **AARE-apdu** with a) **result** component set to **rejected-permanent**; b) the **result-source-diagnostics** taking the **acse-service-user** alternative with the value **no-reason-given**; c) the **OSI-AssoRsp data** value taken the **osiDiag** alternative with the value **invalid-indirect-reference**	ITU-T X.227, 9.1 IEC 62351-4:2018/AMD1:2020, 15.3.3	m
3	Continue with the tests described in Table 50			m

6.2.2 Clear Data Transfer

In the following test scenario, the DUT can be either a client or a server.

For resiliency procedures, different tables describe the tests for the client and the server.

Table 18 – Verification of requirements for OSI environment security – Clear Data transfer

No	Test	Expected result	Reference	Required
1	The DUT initiates the association as described in Table 14.			m
2	Make the DUT to initiate a **ClearTransfer**. EnvPDU: see Table 72 SecPDU: see Table 62	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends a **ClearTransfer**: EnvPDU see 10.4 SecPDU: see Table 63	IEC 62351-4:2018/AMD1:2020, 15.4.2 IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.4.2	m

Table 19 – Clear Data Transfer resiliency procedure in OSI environment – Client

No	Test	Expected result	Reference	Required
1	After having received from the DUT a presentation **User-data** with an embedded **ClearTransfer** SecPDU with an embedded PrPDU requiring response, return a presentation **User-data** with an embedded **ClearTransfer** SecPDU with an embedded PrPDU with an invalid **Presentation-context-identifier.**	Return of an OSI-AssoAbr EnvPDU with the osiDiag alternative holding the **invalid-pci** diagnostic code. The received EnvPDU is verified as specified in Table 70.	IEC 62351.4:2018/AMD1:2020, 15.3.4 IEC 62351.4:2018/AMD1:2020, 15.6.3	m
2	Continue with the tests described in Table 52			m

Table 20 – Clear Data Transfer resiliency procedure in OSI environment – Server

No	Test	Expected result	Reference	Required
1	TEQ initiates a clear data transfer with an invalid presentation-context-identifier.	DUT shall reply an ABRT-apdu with **`AssoAbort`** data value taking the osiDiag alternative with an **`invalid-pci`** diagnostic code to be validated as specified in Table 71	IEC 62351-4:2018/AMD1:2020, 15.4.2	m
2	TEQ initiates a clear data transfer with a missing presentation-context-identifier.	DUT shall reply an ABRT-apdu with **`AssoAbort`** data value taking the **`osiDiag`** alternative with a **`protocol-error`** diagnostic code to be validated as specified in Table 71	IEC 62351-4:2018/AMD1:2020, 15.4.2	m
3	Continue with the tests described in Table 51			m

6.2.3 Encrypted Data Transfer

In the following test scenario, the DUT can be either a client or a server.

For resiliency procedures, different tables describe the tests for the client and the server.

Table 21 – Verification of requirements for OSI environment security – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	The DUT initiates the association as described in Table 14			
2	Make the DUT to initiate an **`EncrTransfer`**. EnvPDU: see Table 73 SecPDU: see Table 64	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **`EncrTransfer`**: EnvPDU see Table 73 SecPDU: see Table 65	IEC 62351-4:2018/AMD1:2020, 15.4.3 IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.4.2 IEC 62351-4:2018/AMD1:2020, 10.4.1	m

Table 22 – Resiliency testing for client – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	TEQ initiates an encrypted data transfer with an invalid presentation-context-identifier.	DUT shall reply an ABRT-apdu with **AssoAbort** data value taking the osiDiag alternative with an **invalid-pci** diagnostic code to be validated as specified in Table 70	IEC 62351-4:2018/AMD1:2020, 15.4.3 IEC 62351-4:2018/AMD1:2020, 15.6 IEC 62351-4:2018/AMD1:2020, 15.3.4 IEC 62351-4:2018/AMD1:2020, 14.2.2	m
2	TEQ initiates an encrypted data transfer with a missing presentation-context-identifier.	DUT shall reply an ABRT-apdu with **AssoAbort** data value taking the **osiDiag** alternative with a **protocol-error** diagnostic code to be validated as specified in Table 70.	IEC 62351-4:2018/AMD1:2020, 15.4.3 IEC 62351-4:2018/AMD1:2020, 15.6 IEC 62351-4:2018/AMD1:2020, 14.2.2 IEC 62351-4:2018/AMD1:2020, 15.3.4	m
3	Continue with the tests described in Table 53			m

Table 23 – Resiliency testing for server – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	TEQ initiates a clear data transfer with an invalid presentation-context-identifier.	DUT shall reply an ABRT-apdu with **AssoAbort** data value taking the osiDiag alternative with an **invalid-pci** diagnostic code to be validated as specified in Table 71.	IEC 62351-4:2018/AMD1:2020, 15.4.3 IEC 62351-4:2018/AMD1:2020, 15.6 IEC 62351-4:2018/AMD1:2020, 14.2.2 IEC 62351-4:2018/AMD1:2020, 15.3.4	m
2	TEQ initiates a clear data transfer with a missing presentation-context-identifier.	DUT shall reply an ABRT-apdu with **AssoAbort** data value taking the **osiDiag** alternative with a **protocol-error** diagnostic code to be validated as specified in Table 71.	IEC 62351-4:2018/AMD1:2020, 15.4.3 IEC 62351-4:2018/AMD1:2020, 15.6 IEC 62351-4:2018/AMD1:2020, 14.2.2 IEC 62351-4:2018/AMD1:2020, 15.3.4	m
3	Continue with the tests described in Table 54			m

6.2.4 Rekey

For this test, the maximum time between key refreshments shall be configured to the shortest delay (15 minutes) to accelerate result.

The tester should configure the client and the server for a continuous communication exchange.

Table 24 – Verification of requirements for OSI environment security – Rekey initiated by the client

No	Test	Expected result	Reference	Required
1	The DUT initiates the association as described in Table 14 – 6			
2	The DUT initiates continuous data transfer. The data can be exchanged in encrypted mode as in table 27 or 28 step 2.		IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	m
3 a)	When the delay of 15 minutes is completed, the 61850-client initiate a rekey. Make the DUT to initiate an **`EncrTransfer`**. EnvPDU: Table 73 SecPDU: Table 64 • **`Rekey`** **shall contain** new DH values • The application data is encrypted using a key derived from the old DH value • **`Auth`** calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **`EncrTransfer`**: EnvPDU Table 73 SecPDU: Table 65 • **`changedKey = TRUE`** • The application data is encrypted using a key derived from the old DH value • **`Auth`** calculated using a key derived from the old DH value	IEC 62351-4:2020, 13.3.2	m
3 b)	DUT shall reply with an **`EncrTransfer`**. EnvPDU: Table 73 SecPDU: Table 64 • The application data is encrypted using a key derived from the new DH value. • **`Auth`** calculated using a key derived from the new DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **`EncrTransfer`**: EnvPDU Table 73 SecPDU: Table 65 • The application data is encrypted using a key derived from the new DH value. • **`Auth`** calculated using a key derived from the new DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m

Table 25 – Verification of requirements for OSI environment security – Rekey initiated by the Server

No	Test	Expected result	Reference	Required
1	The TEQ initiates the association as described in Table 14 – 6			
2	The TEQ initiates continuous data transfer. The data can be exchanged in clear or encrypted mode as in table 27 or 28 step 2.		IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	m
3 a)	When the delay of 15 minutes is completed, the 61850 server requests a rekey. Make the DUT to initiate an **EncrTransfer**. EnvPDU:: Table 73 SecPDU: Table 64 • **reqRekey = TRUE** • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: EnvPDU Table 73 SecPDU: Table 65 • **rekey =** new DH values • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3 b)	DUT shall reply with an **EncrTransfer**. EnvPDU:: Table 73 SecPDU: Table 64 **changedKey = TRUE** The application data is encrypted using a key derived from the old DH value Auth calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: EnvPDU Table 73 SecPDU: Table 65 • The application data is encrypted using a key derived from the new DH value • Auth calculated using a key derived from the new DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3 c)	DUT shall reply with an **EncrTransfer**. EnvPDU:: Table 73 SecPDU: Table 64	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: EnvPDU Table 73 SecPDU: Table 65		m

No	Test	Expected result	Reference	Required
	• The application data is encrypted using a key derived from the new DH value • Auth calculated using a key derived from the new DH value	• The application data is encrypted using a key derived from the new DH value • Auth calculated using a key derived from the new DH value		

7 E2E conformity testing in the XMPP environment

7.1 Conformance tables for E2E-XMPP security profile

The following conformance tables (Table 27, Table 28, Table 29, Table 30, Table 31, Table 32, Table 33, Table 34, Table 35 and Table 36 are used to provide an overview and details about the IEC 61850 <Client and/or Server> produce identified as <device ID and name>, with firmware <version>.

The statement shall identify the applicable details required for each of the Test Cases defined in this document that are either:

m: Mandatory support. The item shall be implemented.

c: Conditional support. The item shall be implemented as specified by the condition.

o: Optional support. The item may be but need not be implemented.

i: Out of scope

Table 26 – Base Profile – E2E XMPP Security

		Client	Server	Comments
Base Profiles				
26-1	Server IEC 61850-8-2 Certified	N/A		
26-2	Client IEC 61850-8-2 Certified		N/A	

Table 27 – Protocol Handshake – E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
IEC 61850 Application association					
27-1	Association Conformance Block Supported	TP			When supported completion of Table 28-1 toTable 28-3 is required to state support or non-support

Table 28 – IEC 61850 Application Association – E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
IEC 61850 Application association					
28-1	Associate	TP			
28-2	Abort	TP	C1		
28-3	Release	TP	C1		
C1: At least Abort or Release shall be supported.					

Table 29 – EnvPDU Parameters– E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
OSI EnvPDU Parameters					
29-1	assoID	TP			Value used for the test session as defined in IEC 62351-4:2020, 13.3.1.1e)

Table 30 – EnvPDU Supported– E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
OSI EnvPDU Supported					
30-1	OSI EnvPDU Supported according to IEC 62351-4	TP			When supported completion of Table 31-1 to of Table 31-9 is required to state support or non-support

Table 31 – SecPDU Subclasses– E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
XMPP EnvPDU Subclass Supported					
31-1	iq stanza HandshakeReq	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-2	iq stanza HandshakeACC	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-3	iq stanza Applicationfeject	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-4	iq stanza HandshakeSecReject	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-5	iq stanza ReleaseReq	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-6	iq stanza ReleaseRsp	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-7	iq stanza ClearTransfer	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-8	iq stanza EncrTransfer	TP			IEC 62351-4:2018/AMD1:2020, 16.2
31-9	message stanza HandshakeSecAbort	TP			IEC 62351-4:2018/AMD1:2020, 16.3
31-10	message stanza DtSecAbort	TP			IEC 62351-4:2018/AMD1:2020, 16.3
31-11	message stanza ApplAbort	TP			IEC 62351-4:2018/AMD1:2020, 16.3
31-12	message stanza ClearTransfer	TP			IEC 62351-4:2018/AMD1:2020, 16.3
31-13	message stanza EncrTransfer	TP			IEC 62351-4:2018/AMD1:2020, 16.3

To be specified by referencing specification. At least one row shall specify "m" for both client and server.

Table 32 – Encryption – E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
Mode of encryption					
32-1	Use of authenticated encryption (AE)	TP			Use of single algorithm for encryption and integrity
32-2	Non-use AE	TP			Non-use of encryption or separate algorithms for encryption and integrity

Table 33 – Cryptographic algorithms – E2E XMPP Security

	Services		AA: TP	Client (C)	Server (S)	Comments
Public-key algorithms						
33-1	rsaEncryptionAlgorithm		TP			Mandatory
33-2	ecPublicKey	secp256r1	TP			Mandatory
		brainpoolP256r1	TP			Mandatory
Signature algorithms						
33-3	`sha256WithRSAEncryptionAlgorithm`		TP			Mandatory
33-4	ecdsa-with-SHA256-Algorithm		TP			Mandatory
Symmetric encryption algorithm						
33-5	aes128-CBC		TP			C1
33-6	aes256-CBC		TP			C1
Authenticated encryption algorithms						
33-7	aes128- GCM		TP			C2
33-8	aes256- GCM		TP			C2
Integrity check value algorithms						
33-9	hmacWithSHA256		TP			C3
33-10	aes128-GCM		TP			C3
33-11	aes256-GCM		TP			C3

C1: Shall be "m" if E2E security with encryption is declared and non-use of authenticated encryption is declared. Otherwise, it shall be "i".

C2: Shall be "m" if E2E security with encryption is declared and use of authenticated encryption is declared. Otherwise, it shall be "i"

C3: Shall be "m" if non-use of authenticated encryption but integrity only **is** declared (see Table 33). Otherwise, it shall be "i".

Table 34 – XMPP – E2E XMPP Security

	Services	AA: TP	Client (C)	Server (S)	Comments
XMPP Parameters					
34-1	61850 Client JID	TP			
34-2	61850 Server JID	TP			
34-3	Domain name	TP			

Table 35 – XMPP– E2E XMPP Security

OSI model layer	Specification			m/o
Service and protocols for client/server communication E2E XMPP security				
	Name	**Service specification**	**Protocol specification**	
Application	Manufacturing Message Specification	ISO 9506-1:2003	ISO 9506-2:2003	m
	MMS end-to-end security	IEC 62351-4:2020	IEC 62351-4:2018/AMD1:2020	m
Presentation	Abstract Syntax	ISO/IEC 8824-1:2008	ITU X.693 (XER)	m
Session	Association context	IEC 62351-4:2020		m
Association Context provides an alternative mapping for M-Services of ISO 9506-2 to end-to-end security and XMPP				

Table 36 – XMPP T-profile – E2E XMPP Security

OSI Model Layer	Specification		m/o
Service and protocols for client/server XMPP T-Profile			
	Name	**Service specification** / **Protocol specification**	
Transport	XMPP	RFC 6120 , RFC 6121, RFC 6122, XEP-0198, XEP-0199	m
	SASL	RFC 4422	m
	TLS	RFC 5246, IEC 62351-6	m
	Transmission Control Protocol (TCP)	RFC 793	m
Network	Internet Control Message Protocol (ICMP)	RFC 792	m
	Internet Protocol	RFC 791	c1, c2
	IPv6	RFC 2460	c1, c2
c1: shall be one or both for XMPP clients c2: mandatory for XMPP servers			

7.2 E2E Test Procedures for XMPP environment

7.2.1 Association Management

The test procedure describes how to validate the initial connection between a client and a server.

The normal result of this test procedure is a successful connection without any exception.

The tester will need to define the high-level test procedure that will initiate the handshake process.

During the following tests, the testers will be able to diagnose using the approach described in Table 2.

Table 37 – Verification of client handshake request procedure in XMPP environment

No	Test	Expected result	Reference	Required
1	Make the DUT to initiate an association. **`iq stanza "set"`** 1) EnvPDU: Table 76 2) SecPDU Table 55	TEQ shall validate the received PDU. 1) If the PDU does not contain error, a) TEQ sends association confirmation **`iq stanza "result"`** i) EnvPDU Table 77 ii) SecPDU Table 56 b) The DUT shall indicate successful connection 2) If the PDU contains error, the test fails.	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.1.4	m
2	DUT to release the association issuing **`ReleaseReq`**. **`iq stanza "set"`** 1) EnvPDU: Table 76 2) SecPDU: Table 66	TEQ shall valid the received PDU. 1) If the PDU does not contain error, a) TEQ sends release response **`iq stanza "result"`** i) EnvPDU: Table 77 ii) SecPDU: Table 67 b) The DUT shall indicate successful connection 2) If the PDU contains error, the test fails	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.1.11 IEC 62351-4:2018/AMD1:2020, 13.3.3	m

Table 38 – Verification of server handshake request procedure in XMPP environment

No	Test	Expected result	Reference	Required
1	Make the TEQ to initiate an association. **`iq stanza "set"`** 1) EnvPDU: see component description in Table 76 2) SecPDU see component description in Table 55	DUT shall validate the received PDU. 1) If the PDU does not contain error, a) DUT sends association confirmation **`iq stanza "result"`** i) EnvPDU Table 77 ii) SecPDU Table 56 b) The TEQ shall validate and indicate successful connection 2) If the PDU contains error, the test fails.	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.1.4	m
2	TEQ to release the association issuing **`ReleaseReq`**. **`iq stanza "set"`** 1) EnvPDU: Table 76 2) SecPDU: Table 66	DUT shall valid the received PDU. 1) If the PDU does not contain error, a) DUT sends release response **`iq stanza "result"`** i) EnvPDU: Table 77 ii) SecPDU: Table 67 b) The DUT shall indicate successful connection 2) If the PDU contains error, the test fails	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.1.11 IEC 62351-4:2018/AMD1:2020, 13.3.3	m

Table 39 describes the tests to verify how the DUT (client) reacts to error conditions. This table includes the tests to be done at the environment level. Tests for secure environment are defined in Table 49

Table 39 – Handshake request resiliency procedure in XMPP environment – Client

No	Test	Expected result	Reference	Required
1	Do the tests described in Table 49			m

Table 40 describes the tests to verify how the DUT (client) reacts to error conditions. This table includes the tests to be done at the environment level. Tests for secure environment are defined in Table 50.

Table 40 – Handshake request resiliency procedure in XMPP environment – Server

No	Test	Expected result	Reference	Required
3	Do the tests described in Table 50			m

7.2.2 Clear Data Transfer

In the following test scenario, the DUT can be a client or a server

`iq stanza "set"` or `"get"` can be used to initiate data transfer from the server.

Table 41 – Verification of requirements for XMPP environment security – Clear Data transfer

No	Test	Expected result	Reference	Required
1	The DUT initiates the association as described in 10.3			
2	Make the DUT to initiate a `ClearTransfer`. `iq stanza "set"` or `"get"` EnvPDU: Table 78 SecPDU: Table 62	TEQ shall validate the received PDU. If the PDU does not contain error, TEQ sends a clear transfer `iq stanza "result"` EnvPDU Table 79 SecPDU: Table 63	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.4.2	m

Table 42 – Clear Data Transfer resiliency procedure in XMPP environment – Server

No	Test	Expected result	Reference	Required
1	Do the tests described in Table 51			m

Table 43 – Clear Data Transfer resiliency procedure in XMPP environment – Client

No	Test	Expected result	Reference	Required
1	Do the tests described in Table 52			m

7.2.3 Encrypted Data Transfer

Table 44 – Verification of requirements for XMPP environment security – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	The DUT initiates the association as described in Table 39			m
2	DUT to initiate a **`EncrTransfer`**. **`iq stanza "set"`** or **`"get"`** EnvPDU: Table 78 SecPDU Table 64	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **`EncrTransfer`**: **`iq stanza "result"`** EnvPDU Table 79 SecPDU Table 65	IEC 62351-4:2018/AMD1:2020, 16.2 IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.4.2	m

Table 45 – Resiliency testing for client – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	Do the tests described in Table 53			m

Table 46 – Resiliency testing for server – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	Do the tests described in Table 54			m

7.2.4 Rekey

For this test, the maximum time between key refreshments shall be configured to the shortest delay (15 minutes) to accelerate result.

The tester should configure the client and the server for a continuous communication exchange.

Table 47 – Verification of requirements for XMPP environment security – Rekey initiated by the client

No	Test	Expected result	Reference	Required
1	The 61850-client initiates the association as described in clause 10.3			m
2	The 61850-client initiates continuous data transfer. The data can be exchanged in encrypted mode as in table 27 or 28 step 2.		IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	m
3 a)	When the delay of 15 minutes is completed, the 61850-client initiate a rekey. Make the DUT to initiate a **EncrTransfer**. **iq stanza "set"** or **"get"** EnvPDU: Table 78 SecPDU: Table 64 • **Rekey shall contain** new DH values • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: **iq stanza "result"** EnvPDU EnvPDU Table 79 SecPDU: Table 65 • **changedKey = TRUE** • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3 b)	DUT shall reply with an **EncrTransfe** **iq stanza "set"** or **"get"** EnvPDU: Table 78 SecPDU: Table 64 • The application data is encrypted using a key derived from the new DH value • **Auth** calculated using a key derived from the new DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: **iq stanza "result"** EnvPDU Table 79 SecPDU: Table 65 • The application data is encrypted using a key derived from the new DH value • **Auth** calculated using a key derived from the new DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
4	The DUT release the association			m

Table 48 – Verification of requirements for XMPP environment security – Rekey initiated by the server

No	Test	Expected result	Reference	Required
1	The 61850-client initiates the association as described in clause 10.3			m
2	The 61850-client initiates continuous data transfer. The data can be exchanged in encrypted mode as in table 27 or 28 step 2.		IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	m
3 a)	When the delay of 15 minutes is completed, the 61850 server requests a rekey. **iq stanza "result"** EnvPDU: Table 78 SecPDU: Table 64 • **reqRekey = TRUE** • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: **iq stanza "set"** or **"get"** EnvPDU Table 79 SecPDU: Table 65 • **rekey** = new DH values • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3 b)	DUT shall reply with an **EncrTransfer**. **iq stanza "result"** EnvPDU: Table 78 SecPDU: Table 64 • **changedKey = TRUE** • The application data is encrypted using a key derived from the old DH value • **Auth** calculated using a key derived from the old DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: **iq stanza "set"** or **"get"** EnvPDU Table 79 SecPDU: Table 65 • The application data is encrypted using a key derived from the new DH value • **Auth** calculated using a key derived from the new DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m

No	Test	Expected result	Reference	Required
3 c)	DUT shall reply with an **EncrTransfer**. **iq stanza "result"** EnvPDU EnvPDU: Table 78 SecPDU: Table 64 • The application data is encrypted using a key derived from the new DH value • **Auth** calculated using a key derived from the new DH value	TEQ shall valid the received PDU. If the PDU does not contain error, TEQ sends an **EncrTransfer**: **iq stanza "set"** or **"get"** EnvPDU Table 79 SecPDU: Table 65 • The application data is encrypted using a key derived from the new DH value • **Auth** calculated using a key derived from the new DH value	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
4	The DUT release the association 3			m

8 E2E Resiliency test procedures

8.1 General

This clause describes the tests that should be done to validate the resiliency of E2E security profile.

The tests in this clause are independent of the EnvPDU.

8.2 Association Management Resiliency Testing

Table 49 – Handshake request resiliency procedure – Client

No	Test	Expected result	Reference	Required
1	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **sigAlg** component of ClearToken1 holding a value different from the one specified in the **algo** component of **Signature** data value.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the diag component absent to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a) IEC 62351-4:2018/AMD1:2020, 13.4.1 a) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 1)	m
2	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with a missing mandatory component of **ClearToken1**.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding a **protocol-error** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 2)	m
3	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **pkcert** component holding an invalid public-key certificate.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **invalid-public-key-certificate** diagnostic code to be checked as specified in Table 59.	EC 62351-4:2018/AMD1:2020, 13.3.1.1 k) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 9)	m
4	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **pkcert** component holding a valid public-key certificate but the senders address is different from the subject component of the public-key certificate.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component absent to be checked as specified in Table 59.	EC 62351-4:2018/AMD1:2020, G.6 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 1)	m
5	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a)	m

No	Test	Expected result	Reference	Required
	with a digital signature algorithm not supported by the client (DUT).	**invalid-signatureAlgorithm** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 4)	
6	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **version** component having a value not among those suggested by the client (DUT).	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **unexpected-version** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 5)	m
7	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **invalid-time-value** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 11)	m
8	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **time** and **assoID** components having the same values as in a previous test.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component absent to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 1)	m
9	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with the **dHKey** component having the **DiffieHellmanSet** data value having a **groupId** component different from those supported by the client (DUT).	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **illegal-dhGroup-selected** diagnostic code to be checked as specified in Table 59	IEC 62351-4:2018/AMD1:2020, 13.3.1.2 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 13)	m
10	After having received a valid handshake request, send an EnvPDU with an embedded **HandshakeAcc** SecPDU	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **hmac-algorithm-not-supported**	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 h)	m

No	Test	Expected result	Reference	Required
	with the **hmac** component with a HMAC algorithm not supported by the client (DUT).	diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 6)	
11	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU including an **encr-mode.non-aea** component, send an EnvPDU with an embedded **HandshakeAcc** SecPDU with an **encr-mode.aea** component.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **aea-algorithms-not-supported** diagnostic code to be checked as specified in Table 59	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 16)	m
12	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including the **encr** component holding one or more symmetric-key algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** with the **encr** component specifying a symmetric-key algorithm not present in the corresponding **HandshakeReq** SecPDU.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **invalid-encryption-algorithm** diagnostic code to be checked as specified in Table 59.	IEC 62351-4 2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 24)	m
13	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including the **encr** component holding one or more symmetric-key algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** with the **encr** component specifying multiple symmetric-key algorithms.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding a **single-encrypt-algo-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 25)	m
14	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including the **encr** component holding one or more symmetric-key algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** with the **encr** component specifying an empty set 0f symmetric-key algorithms.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding a **single-encrypt-algo-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 25)	m
15	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including holding one or more	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding an **icv-**	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i)	m

No	Test	Expected result	Reference	Required
	ICV algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** with an ICV algorithm not included in the corresponding **HandshakeReq** SecPDU.	**algorithms-not-supported** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 14)	
16	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including holding one or more ICV algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** holding multiple ICV algorithms.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding a **single-icv-algo-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 26)	m
17	After having received a valid handshake request with an embedded **HandshakeReq** SecPDU specifying **encr-mode.non-aea** including holding one or more ICV algorithms, send an EnvPDU with an embedded **HandshakeAcc** SecPDU the **encr-mode.non-aea** holding an empty set of ICV algorithms.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **diag** component holding a **single-icv-algo-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 15.3.1.1 g) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 26)	m
18	After having received a valid handshake request specifying **encr-mode.non-aea** including the **encr** component, send an **AARE-apdu** with the **result** component set to **accepted** and with an embedded **HandshakeAcc** SecPDU with the **encr-mode.non-aea** with the **encr** component excluded.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **encryption-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 15.3.1.1 g) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 8)	m
19	After having received a valid handshake request specifying **encr-mode.non-aea** without including the **encr** component, send an EnvPDU an embedded **HandshakeAcc** SecPDU with the **encr-mode.aea** component included.	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **encryption-not-required** diagnostic code to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 15.3.1.1 g) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.2 7)	m
20	After having received a valid handshake request specifying **encr-mode.non-aea** without including the **encr** component, send an EnvPDU with an embedded	An EnvPDU with an embedded **HandshakeSecAbort** SecPDU with the **encryption-not-required** diagnostic code. This SecPDU to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 15.3.1.1 g) IEC 62351-4:2018/AMD1:2020, 13.1.7	m

No	Test	Expected result	Reference	Required
	HandshakeAcc SecPDU with the **encr-mode.non-aea** with the **encr** component included.		IEC 62351-4:2018/AMD1:2020, 14.2.2 7)	
21	After having received a valid handshake request, issue an EnvPDU with an embedded **HandshakeReq** SecPDU having the **applProtected** bit set in the **confidentialityParms** component.	An EnvPDU with an embedded **HandshakeSecAbort** with the **diag** component holding an **encryption-not-required** diagnostic code. This SecPDU to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.4 IEC 62351-4:2018/AMD1:2020, 13.3.1.1 j) IEC 62351-4:2018/AMD1:2020, 14.2.2 7)	m
22	Knowing that the server require encryption, issue an EnvPDU with an embedded **HandshakeReq** SecPDU having the **applProtected** bit not set in the **confidentialityParms** component.	An EnvPDU with an embedded **HandshakeSecAbort** with the **diag** component holding an **encryption-required** diagnostic code. This SecPDU to be checked as specified in Table 59.	IEC 62351-4:2018/AMD1:2020, 13.3.1.4 IEC 62351-4:2018/AMD1:2020, 13.3.1.1 j) IEC 62351-4:2018/AMD1:2020, 14.2.2 8)	m

Table 50 – Handshake request resiliency procedure – Server

No	Test	Expected result	Reference	Required
1	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with a **pp** component that species a protected protocol different from the one used during the testing.	An EnvPDU with a valid embedded **HandshakeSecReject** SecPDU with a **protected-protocol-not-supported** diagnostic code. This SecPDU to be checked as specified in Table 58.	IEC 62351-4:2018/AMD1:2020, 13.1.3 a) IEC 62351-4:2018/AMD1:2020, 14.2.1, 3)	m
2	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **sigAlg** component of ClearToken1 holding a value different from the one specified in the **algo** component of **Signature** data value.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the diag component **no-reason-given** to be checked as specified in Table 58.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a) IEC 62351-4:2018/AMD1:2020, 13.4.1 a) IEC 62351-4:2018/AMD1:2020, 14.2.1, 1)	m
3	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with a missing mandatory component of the **ClearToken1** data value.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding a **protocol-error** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 2)	m
4	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **pkcert** component holding an invalid public-key certificate.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the diag component holding an **invalid-public-key-certificate** diagnostic code to be checked as specified in 9.4.	EC 62351-4:2018/AMD1:2020, 13.3.1.1 k) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 9)	m
5	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **pkcert** component holding a valid public-key certificate but the senders address is different from the **subject** component of the public-key certificate.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component **no-reason-given** to be checked as specified in 9.4.	EC 62351-4:2018/AMD1:2020, G.6 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 1)	m

No	Test	Expected result	Reference	Required
6	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with a digital signature algorithm not supported by the server (DUT).	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding an **invalid-signatureAlgorithm** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 4)	m
7	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **version** component having a value not among those suggested by the client (DUT).	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding an **unexpected-version** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 5)	m
8	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding an **invalid-time-value** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 11)	m
9	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **time** and **assoID** components having the same values as in a previous test.	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component **no-reason-given** to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 1)	m
10	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **dHKey** component having the **DiffieHellmanSet** data value having a **groupId** component value not supported by the server (DUT).	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding a **dhGroup-not-supported** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.2 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 12)	m

No	Test	Expected result	Reference	Required
11	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **hmac** component holding a HMAC algorithm not supported by the server (DUT).	An EnvPDU with an embedded **HandshakeSecReject** SecPDU with the **diag** component holding a **hmac-algorithm-not-supported** diagnostic code to be checked as specified in 9.4.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 6)	m
12	Knowing that the server does not support or do not want to support AEAD algorithms, issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **encr-mode.aea** component present with one or more AEAD algorithms	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **aea-algorithms-not-supported** diagnostic code. This SecPDU to be checked as specified in Table 58.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.1) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 16)	m
13	Knowing that the server does not support or do not want to support encryption, issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **encr-mode.aea** component present with one or more AEAD algorithms	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **aea-select-but-encryp-not-supported** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.1) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 20)	m
14	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **encr-mode.aea** component present with one or more AEAD algorithms not supported by the server	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **aea-algorithms-not-supported** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.1) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 16)	m
15	Knowing that the server requires use of AEAD, issue an EnvPDU with a valid embedded valid **HandshakeReq** SecPDU with the **encr-mode.non-aea** component present.	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **aea-is-required** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2.ii) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 19)	m

No	Test	Expected result	Reference	Required
16	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with the **encr-mode.non-aea** component present with ICV algorithms known not to be supported by the server.	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **icv-algorithms-not-supported** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2.ii) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 14)	m
17	Knowing that the server does not support or do not want to support encryption, issue an EnvPDU with an embedded **HandshakeReq** SecPDU having the **applProtected** bit set in the **confidentialityParms** component.	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **encryption-not-required** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 j) IEC 62351-4:2018/AMD1:2020, 13.3.1.4 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 7)	m
18	Knowing that the server require encryption, issue an EnvPDU with an embedded **HandshakeReq** SecPDU having the **applProtected** bit not set in the **confidentialityParms** component.	An EnvPDU with an embedded **HandshakeSecReject** with the **diag** component holding an **encryption-required** diagnostic code. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 j) IEC 62351-4:2018/AMD1:2020, 13.3.1.4 IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 8)	m
19	Issue an EnvPDU with a valid embedded **HandshakeReq** SecPDU with the **encr-mode.non-aea** component present with multiple supported symmetric key algorithms in the **encr** component.	An EnvPDU with a valid embedded **HandshakeAcc** SecPDU with the **encr-mode-aeanot-supported** component present with a single symmetric key algorithm, which should be the first one presented in the **HandshakeReq** SecPDU. This SecPDU to be checked as specified in 9.2.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2.i) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 18)	m

No	Test	Expected result	Reference	Required
20	Issue an EnvPDU with an embedded **HandshakeReq** SecPDU with a **time** component that is more than 10 minutes off the current time.	An EnvPDU with a valid embedded **HandshakeSecReject** SecPDU with an **invalid-time-value** diagnostic code. This SecPDU to be checked as specified in Table 58	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.7 IEC 62351-4:2018/AMD1:2020, 14.2.1, 11)	m

8.3 Clear Data Transfer Resiliency

For the tests described in Table 51, TEQ is a client and DUT is a server

Table 51 – Clear Data Transfer resiliency – Server

No	Test	Expected result	Reference	Required
1	Make the TEQ to send an EnvPDU with an embedded **ClearTransfer** SecPDU with a missing **ClearToken2** mandatory component.	DUT to return an EnvPDU with an embedded **DtSecAbort** with the **diag** component holding a **protocol-error** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 2) IEC 62351-4:2018/AMD1:2020, 14.4	m
2	Make the TEQ to send an EnvPDU with an embedded **ClearTransfer** SecPDU with a **version** component holding a value different from the one included in the corresponding **HandshakeAcc** SecPDU	DUT to return an EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-version** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 3)	m

No	Test	Expected result	Reference	Required
			IEC 62351-4:2018/AMD1:2020, 14.4	
3	Make the TEQ to send an EnvPDU with an embedded **`EncrTransfer`** SecPDU..	DUT to return an EnvPDU with an embedded **`DtSecAbort`** with the **`diag`** component holding an **`encryption-not-selected`** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 4) IEC 62351-4:2018/AMD1:2020, 14.4	m
4	Make the TEQ to send an EnvPDU with an embedded **`ClearTransfer`** SecPDU with an invalid sequence number.	DUT to return an EnvPDU with an embedded **`DtSecAbort`** with the **`diag`** component holding an **`invalid-sequence-number`** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 9) IEC 62351-4:2018/AMD1:2020, 14.4	m

No	Test	Expected result	Reference	Required
5	Make the TEQ to send an EnvPDU with an embedded **ClearTransfer** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	DUT to return an EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-time-value** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 8) IEC 62351-4:2018/AMD1:2020, 14.4	m
6	Make the TEQ to send an EnvPDU with an embedded **ClearTransfer** SecPDU with the **time** component and the **seq** component having the same value as in a previous received SecPDU.	DUT to return an EnvPDU with an embedded **DtSecAbort** with the **diag** component **no-reason-given**. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 1) IEC 62351-4:2018/AMD1:2020, 14.4	m

For the tests described in Table 52, DUT is a client and TEQ is a server

Table 52 – Clear Data Transfer resiliency – Client

No	Test	Expected result	Reference	Required
1	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with a missing **ClearToken2** mandatory component	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding a **protocol-error** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8	m

No	Test	Expected result	Reference	Required
			IEC 62351-4:2018/AMD1:2020, 14.2.2, 2) IEC 62351-4:2018/AMD1:2020, 14.4	
2	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with a **version** component holding a value different from the one included in the corresponding **HandshakeAcc** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-version** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 3) IEC 62351-4:2018/AMD1:2020, 14.4	m
3	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **encryption-not-selected** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 4) IEC 62351-4:2018/AMD1:2020, 14.4	m
4	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with an invalid sequence number.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-sequence-number** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 9)	m

No	Test	Expected result	Reference	Required
			IEC 62351-4:2018/AMD1:2020, 14.4	
5	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-time-value** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 8) IEC 62351-4:2018/AMD1:2020, 14.4	m
6	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with the **time** component and the **seq** component having the same value as in a previous received SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component **no-reason-given**. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 1) IEC 62351-4:2018/AMD1:2020, 14.4	m
7	Make the client submit an EnvPDU with an embedded valid **ClearTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU with the **changedKey** component included without have received an outstanding **rekey** request	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-changedKey** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 12) IEC 62351-4:2018/AMD1:2020, 14.4	m

8.4 Encrypted Data Transfer Resiliency

Table 53 – Resiliency testing for client – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **rEncrTransfer** SecPDU with a missing **ClearToken2** mandatory component	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding a **protocol-error** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 2) IEC 62351-4:2018/AMD1:2020, 14.4	m
2	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with a **version** component holding a value different from the one included in the corresponding **HandshakeAcc** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-version** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 3) IEC 62351-4:2018/AMD1:2020, 14.4	m
3	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **encryption-required** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 5) IEC 62351-4:2018/AMD1:2020, 14.4	m

No	Test	Expected result	Reference	Required
4	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with an invalid sequence number.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-sequence-number** diagnostic code. This SecPDU to be checked as specified Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 9) IEC 62351-4:2018/AMD1:2020, 14.4	m
5	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-time-value** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 8) IEC 62351-4:2018/AMD1:2020, 14.4	m
6	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with the **time** component and the **seq** component having the same value as in a previous received SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component **no-reason-given**. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 1) IEC 62351-4:2018/AMD1:2020, 14.4	m
7	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-changedKey** diagnostic code.	IEC 62351-4:2018/AMD1:2020, 13.2.3	m

No	Test	Expected result	Reference	Required
	embedded **EncrTransfer** SecPDU with the **changedKey** component included without have received an outstanding **rekey** request	This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 12) IEC 62351-4:2018/AMD1:2020, 14.4	

Table 54 – Resiliency testing for server – Encrypted data transfer

No	Test	Expected result	Reference	Required
1	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **rEncrTransfer** SecPDU with a missing **ClearToken2** mandatory component	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding a **protocol-error** diagnostic code. This SecPDU to be checked as specified in Table 60	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 2) IEC 62351-4:2018/AMD1:2020, 14.4	m
2	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with a **version** component holding a value different from the one included in the corresponding **HandshakeAcc** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-version** diagnostic code. This SecPDU to be checked as specified in Table 60.	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 3) IEC 62351-4:2018/AMD1:2020, 14.4	m

No	Test	Expected result	Reference	Required
3	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **ClearTransfer** SecPDU.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **encryption-required** diagnostic code. This SecPDU to be checked as specified in Table 60.	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 5) IEC 62351-4:2018/AMD1:2020, 14.4	m
4	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with an invalid sequence number.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-sequence-number** diagnostic code. This SecPDU to be checked as specified in Table 60.	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 9) IEC 62351-4:2018/AMD1:2020, 14.4	m
5	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with the **time** component having a value more than 10 minutes from the adjusted current time.	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **invalid-time-value** diagnostic code. This SecPDU to be checked as specified in Table 60.	IEC 62351-4: 2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 8) IEC 62351-4:2018/AMD1:2020, 14.4	m
6	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an	An EnvPDU with an embedded **DtSecAbort** with the **diag** component **no-reason-given**.	IEC 62351-4:2018/AMD1:2020, 13.2.3	m

No	Test	Expected result	Reference	Required
	embedded **EncrTransfer** SecPDU with the **time** component and the **seq** component having the same value as in a previous received SecPDU.	This SecPDU to be checked as specified in Table 60-	IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 1) IEC 62351-4:2018/AMD1:2020, 14.4	
7	Make the client submit an EnvPDU with an embedded valid **EncrTransfer** SecPDU with an embedded PrPDU requiring a response. When this request is received by the TEQ, send an EnvPDU with an embedded **EncrTransfer** SecPDU with the **changedKey** component included without have received an outstanding **rekey** request	An EnvPDU with an embedded **DtSecAbort** with the **diag** component holding an **unexpected-changedKey** diagnostic code. This SecPDU to be checked as specified in Table 60.	IEC 62351-4:2018/AMD1:2020, 13.2.3 IEC 62351-4:2018/AMD1:2020, 13.3.2 IEC 62351-4:2018/AMD1:2020, 13.1.8 IEC 62351-4:2018/AMD1:2020, 14.2.2, 12) IEC 62351-4:2018/AMD1:2020, 14.4	m

9 E2E security subclass (SecPDU)

9.1 E2E Handshake request subclass

This subclass is invoked when the control function requests an association establishment. The input consists of:

- if relevant, a PrPDU to be included in the handshake request SecPDU;
- the cryptographic algorithms to be used and proposed. Only cryptographic algorithms recognized by IEC 62351-4 are allowed.;
- the Diffie-Hellman algorithm parameters to be used;
- whether encryption shall be supported;
- if encryption, whether authenticated encryption shall be used or not;
- the public-key certificate to be included;

- if relevant, the certification path to be included; and
- if relevant, an attribute certificate.

Table 55 – E2E handshake request subclass

No	Component	Definition	Reference	Required
1	**pp**	Check if the application protocol to be protected is recognized and supported.	IEC 62351-4:2018/AMD1:2020, 13.1.3 a)	m
2	**tbs**	Tbs includes part of the PDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.3 b)	m
3	**token1**	Shall hold the ClearToken1 components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.1	m
4	**sigAlg**	It shall be checked that this component holds a digital signature algorithm, and that this algorithm is among those algorithms that were declared as supported.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a)	m
5	**pkCert**	The validity of the public-key certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 b)	m
6	**certPath**	If present, the validity of the CA certificates in the **certPath** component shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 c)	c1
7	**version**	Check that bit 0 of the bit string is set and no other bits in the bit string is set.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d)	m
8	**assoID**	Check that the assoID is conforming to the requirement specified in IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) for the client.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e)	m
9	**dHKey**	Diffie-Hellman specification.	IEC 62351-4:2018/AMD1:2020, 13.3.1.2	m
10	**groupId**	Check that either group 14, 23 or 28 is specified.	IEC 62351-4:2018/AMD1:2020, 13.3.1.2 a)	m
11	**dhPublicKey**	Check the validity of the Diffie-Hellman public key with respect to the selected group.	IEC 62351-4:2018/AMD1:2020, 13.3.1.3 b)	m
12	**hmac**	It shall be checked whether the suggested HMAC algorithms is supported.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 h)	m

No	Component	Definition	Reference	Required
13	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the current local time value plus/minus 5 minutes.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
14	**encr-mode**	General encryption specifications	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i)	m
15	**aea**	The presence shall be checked and if present, it shall be checked whether at least one of the suggested authenticated encryption with associated data (AEAD algorithms is supported).	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.1)	c2
16	**non-aea**	The presence shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2)	c3
17	**encr**	It shall be checked whether at least one of the suggested symmetric key algorithms is supported.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i. 2. i)	c4
18	**icvAlgID**	It shall be checked whether at least one of the suggested ICV algorithms is supported.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i. 2. ii)	c3
19	**confParams**	Check that the **applProtected** bit is not set when encryption is not selected and that it is set when encryption is selected.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.3.1.4	m
20	**attCert**	The validity of the attribute certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 k)	c5
21	**applData**	If the protected protocol has association initialization values, this component shall hold the PrPDU holding these components of this PrPDU shall be checked against the configuration parameters of that PrPDU (if such test specification exists)	IEC 62351-4:2018/AMD1:2020, 13.1.3 b 2)	c6
22	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.3 c) IEC 62351-4:2018/AMD1:2020, 13.4.1	m
23	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m

No	Component	Definition	Reference	Required
24	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present. c2: The component shall be present if the DUT has declared the use of AEAD. Otherwise, it shall be absent.. c3: The component shall be present if the DUT has declared the non-use of AEAD. Otherwise, it shall be absent. c4: The component shall be present if the DUT has declared the non-use of AEAD and use of encryption. Otherwise, it shall be absent. c5: The component shall be present if the DUT has declared inclusion of an attribute certificate. Otherwise, it shall be absent. c6: This component shall be present if the protected protocol under test requires initialization information. Otherwise, it shall be absent.				

9.2 E2E handshake accept subclass

This subclass is invoked when a received handshake request has been accepted. The input consists of:

- if relevant, a PrPDU to be included in the handshake accept SecPDU;
- which of the proposed cryptographic algorithms are selected;
- copy of some handshake request component, such a used cryptographic algorithms, and Diffie-Hellman specifications
- the public-key certificate to be included; and
- if relevant, the certification path to be included.

Table 56 – E2E handshake accept subclass.

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the SecPDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.4 a)	m
2	**token1**	Shall hold the ClearToken1 components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.1	m
3	**sigAlg**	Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 a)	m

No	Component	Definition	Reference	Required
4	**pkCert**	The validity of the public-key certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 b)	m
5	**certPath**	If present, the validity of the CA certificates in the **certPath** component shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 c)	c1
6	**version**	Check that bit 0 of the bit string is set and no other bits in the bit string is set.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d)	m
7	**assoID**	Check that the assoID is conforming to the requirement specified in IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) for the server.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e)	m
8	**dHKey**	Diffie-Hellman specification.	IEC 62351-4:2018/AMD1:2020, 13.3.1.2	m
9	**groupId**	Check that the same group is specified as in the corresponding **HandshakeReq** SecPDU..	IEC 62351-4:2018/AMD1:2020, 13.3.1.2 a)	m
10	**dhPublicKey**	Check the validity of the Diffie-Hellman public key with respect to the selected group.	IEC 62351-4:2018/AMD1:2020, 13.3.1.3 b)	m
11	**hmac**	It shall be checked whether the suggested HMAC algorithms is the same as in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 h)	m
12	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the value supplied in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 f) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
13	**Encr-mode**	General encryption specifications	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i)	m
14	**aea**	Check whether presence or absence is the same as for the corresponding alternative in the corresponding **HandshakeReq** SecPDU. If present, check whether one only one AEAD algorithm is listed and that this algorithm is one of those suggested in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.1)	c2
15	**Non-aea**	Check whether presence or absence is the same as for the corresponding alternative in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i. 2)	c2

No	Component	Definition	Reference	Required
16	**encr**	Check whether presence or absence is the same as for the corresponding component in the corresponding **HandshakeReq** SecPDU. If present, check that only one symmetric key algorithm is listed and that this algorithm is one of those suggested in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2.i)	c3
17	**icvAlgID**	Check whether presence or absence is the same as for the corresponding component in the corresponding **HandshakeReq** SecPDU. If present, check that only one ICV algorithm is listed and that this algorithm is one of those suggested in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i.2.ii)	c2
18	**confParams**	Check that this component has the same value as the corresponding component of the corresponding **HandshakeReq** SecPDU..	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 j) IEC 62351-4:2018/AMD1:2020, 13.3.1.4	m
19	**attCert**	The validity of the attribute certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 k)	c4
20	**applData**	If the protected protocol has association initialization values, this component shall hold the PrPDU holding these components of this PrPDU shall be checked against the configuration parameters of that PrPDU (if such test specification exists)	IEC 62351-4:2018/AMD1:2020, 13.1.3 b. 2)	c5
21	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.3 c) IEC 62351-4:2018/AMD1:2020, 13.4.1	m
22	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
23	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m

c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present.

c2: The component shall be present if the DUT has declared the use of AEAD. Otherwise, it shall be absent.

c3: The component shall be present if the DUT has declared the non-use of AEAD. Otherwise, it shall be absent.

c4: The component shall be present if the DUT has declared the non-use of AEAD and use of encryption. Otherwise, it shall be absent.

No	Component	Definition	Reference	Required
c5: This component shall be present when required by the protected protocol. Otherwise, it shall be absent.				

9.3 E2E Application reject subclass

This subclass is invoked when a received handshake request contains with faulty initialization information for the protected protocol such as:

- the protected protocol has initialization information to be exchanged during the handshake procedure;
- the initialization information is not accepted by the server; and
- information is available that allows bad initialization information to be generated and submitted to the DUT (server) in the handshake request.

The input consists of:

- the PrPDU to be included in the application reject SecPDU;
- signature algorithm copied from handshake request;
- the public-key certificate to be included; and
- if relevant, the certification path to be included.

Table 57 – E2E Application reject subclass

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the SecPDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.5 a)	m
2	**token3**	Shall hold the **ClearToken3** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.3	m
3	**sigAlg**	Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 a)	m
4	**version**	Check that it has the same value as in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 b)	m
5	**assoID**	The presence shall be check according to IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	m
6	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the value supplied in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 d) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
7	**pkCert**	The validity of the public-key certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.3 e)	m
8	**certPath**	If present, the validity of the CA certificates in the **certPath** component shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.3 f)	c1
9	**applData**	A PrPDU shall be present. Analysis of the PrPDU is out of scope of this part of IEC 62351. Analysis should be according to the test specification for the protected protocol.	IEC 62351-4:2018/AMD1:2020, 13.1.5 a.2)	m
10	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.5 b) IEC 62351-4:2018/AMD1:2020, 13.4.1	m

11	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.1.5 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
12	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.1.5 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present..				

9.4 E2E Handshake reject subclass

This subclass is invoked when a received handshake request has been rejected by the protected application.

- the protected protocol has initialization information to be exchanged during the handshake procedure;
- the initialization information is not accepted by the server; and
- information is available that allows bad initialization information to be generated and submitted to the DUT (server) in the handshake request.

The input consists of:

- the PrPDU to be included in the application reject SecPDU;
- signature algorithm copied from handshake request;
- the public-key certificate to be included; and
- if relevant, the certification path to be included.

Table 58 – Server reject of association due to security issues

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the SecPDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.6 a	m
2	**token3**	Shall hold the **ClearToken3** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.3	m
3	**sigAlg**	Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 a)	m
4	**version**	Check that it has the same value as in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 b)	m
5	**assoID**	The presence shall be checking according to IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	m
6	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the value supplied in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 d) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
7	**pkCert**	The validity of the public-key certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.3 e)	m
8	**certPath**	If present, the validity of the CA certificates in the **certPath** component shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.3 f)	c1
9	**diag**	Check that the value is identical to the expected one depending on the type of test	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 2) IEC 62351-4:2018/AMD1:2020, 14.2.1	c2
10	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1	m

No	Component	Definition	Reference	Required
11	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
12	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present. c2: The diag component shall be absent if the exception condition detected by the client should cause an alarm. Otherwise, it shall be present with the appropriate diagnostic code.				

9.5 E2E Handshake security abort subclass

This subclass is invoked when a received handshake request has been rejected due to unaccepted security specifications. The input consists of:

- information about the problem;
- signature algorithm copied from handshake request;
- the public-key certificate to be included; and
- if relevant, the certification path to be included.

Table 59 – Test of client submitted handshake security abort

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the PDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.7	m
2	**token3**	Shall hold the **ClearToken3** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.3	m
3	**sigAlg**	Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 a)	m
4	**version**	Check that it has the same value as in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 b)	m
5	**assoID**	The presence shall be checking according to IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	IEC 62351-4:2018/AMD1:2020, 13.3.3 c)	m
6	**time**	Check that the time value is consistent with the value supplied in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 d) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
7	**pkCert**	Check that the public-key certificate is the same as used in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 e)	m
8	**certPath**	Check that if this component was absent in the corresponding **HandshakeReq** SecPDU, then it is also absent here. If it was present the If it was present in the **HandshakeReq** SecPDU, the check that the sequence of CA certificates is the same as used in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 f)	c1
9	**diag**	Check that the value is identical to the expected one depending on the type of test	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 2) IEC 62351-4:2018/AMD1:2020, 14.2.1	c2
10	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1	m

11	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
12	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.1.6 a. 3) IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present. c2: The diag component shall be absent if the exception condition detected by the client should cause an alarm. Otherwise, it shall be present with the appropriate diagnostic code.				

9.6 E2E Data transfer security abort subclass

This subclass is invoked when a received data transfer has been rejected due to unaccepted security specifications. The input consists of:

- information about the problem;
- signature algorithm copied from handshake request;
- the public-key certificate to be included; and

if relevant, the certification path to be included.

Table 60 – Client or server emitted data transfer security abort

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the PDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.8 a)	m
2	**token3**	Shall hold the **ClearToken3** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.3	m
3	**sigAlg**	Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 a)	m
4	**version**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 b) IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d)	m
5	**assoID**	Check the value is the same as specified in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 c) IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e)	m
6	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the value supplied in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 d) IEC 62351-4:2018/AMD1:2020, 13.1.2..	m
7	**pkCert**	The validity of the public-key certificate shall be checked.	IEC 62351-4:2018/AMD1:2020, 13.3.3 e)	m
8	**certPath**	Check that if this component was absent in the corresponding **HandshakeReq** SecPDU, then it is also absent here. If it was present the If it was present in the **HandshakeReq** SecPDU, the check that the sequence of CA certificates is the same as used in the corresponding **HandshakeReq** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 f)	c1
9	**diag**	Check that the value is identical to the expected one depending on the type of test	IEC 62351-4:2018/AMD1:2020, 13.1.8 a. 2) IEC 62351-4:2018/AMD1:2020, 14.2.12	c2

No	Component	Definition	Reference	Required
10	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.8 b IEC 62351-4:2018/AMD1:2020, 13.4.1	m
11	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component.	IEC 62351-4:2018/AMD1:2020, 13.1.8 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
12	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.1.8 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The component shall be absent if the information is supplied during the engineering process or if the end-entity public-key certificate was issued directly by the trust anchor. Otherwise, it shall be present. c2: The diag component shall be absent if the exception condition detected by the client should cause an alarm. Otherwise, it shall be present with the appropriate diagnostic code.				

9.7 E2E Abort by protected protocol subclass

This subclass is invoked when the protected protocol issues an abort for some reason. The input consists of:

- if relevant, PrPDU providing information the abort reason;
- signature algorithm copied from handshake request;
- the public-key certificate to be included; and
- if relevant, the certification path to be included.

Table 61 – Client or server emitted abort by protected protocol

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the PDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.1.9 a)	m
2	**token3**	Shall hold the **ClearToken3** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.3	m
3	**sigAlg**	For the client: Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeReq** SecPDU. For the server: Checked that this component holds a digital signature algorithm identical to the one specified in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 a)	m
4	**version**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 b) IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d)	m
5	**assoID**	Check the value is the same as specified in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.3 c) IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e)	m
6	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the current local time value plus/minus 5 minutes.	IEC 62351-4:2018/AMD1:2020, 13.3.3 d) IEC 62351-4:2018/AMD1:2020, 13.1.2	m
7	**pkCert**	Check that the end-entity public-key certificate is identical to the one used in the corresponding **HandshakeReq** SecPDU for the client or is identical to the one used in the corresponding **HandshakeAcc** SecPDU for the server.	IEC 62351-4:2018/AMD1:2020, 13.3.3 e)	m
8	**certPath**	For the client: Check that if this component was absent in the corresponding **HandshakeReq** SecPDU, then it is also absent here. If it was present in the **HandshakeReq** SecPDU, the check that the sequence of CA certificates is the same as used in the corresponding **HandshakeReq** SecPDU. For the server: Check that if this component was absent in the corresponding **HandshakeAcc** SecPDU, then it is also absent here. If it was present in the	IEC 62351-4:2018/AMD1:2020, 13.3.3 f) IEC 62351-4:2018/AMD1:2020, 13.3.1.5	m

No	Component	Definition	Reference	Required
		HandshakeAcc SecPDU, the check that the sequence of CA certificates is the same as used in the corresponding **HandshakeAcc** SecPDU.		
9	**applData**	If the protected protocol provides diagnostic, this component shall hold the PrPDU holding this information. This PrPDU shall be checked against the protected protocol specification.	IEC 62351-4:2018/AMD1:2020, 13.1.9 a.2)	c1
10	**sign**	Signature data value	IEC 62351-4:2018/AMD1:2020, 13.1.9 b) IEC 62351-4:2018/AMD1:2020, 13.4.1	m
11	**algo**	It shall be checked that it has the same value as in the **token3.sigAlg** component and that it has the same value is in the corresponding handshake request.	IEC 62351-4:2018/AMD1:2020, 13.1.9 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 a)	m
12	**sign**	The digital signature shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.1.9 b) IEC 62351-4:2018/AMD1:2020, 13.4.1 b)	m
c1: The applData component shall be absent if the exception condition detected by the protected protocol should cause an alarm. Otherwise, it shall be present with the appropriate diagnostic information.				

9.8 E2E Clear data transfer subclass

This subclass is invoked when a data transfer PrPDU to be transmitted in clear has been created. The input consists of:

- the PrPDU to be transmitted;
- the algorithm used for ICV generation;
- if transmitted by the client, whether it is time for renewal of symmetric keys;
- if transmitted by the server, whether changed key indication should be sent; and
- if transmitted by the server, whether a re-key request indication shall be sent.

Table 62 – Client initiated clear data transfer

No	Component	Definition	Reference	Required
1	**tbp**	Tbs includes part of the SecPDU that shall be protected by the ICV	IEC 62351-4:2018/AMD1:2020, 13.2.2 a)	m
2	**token2**	Shall hold the **ClearToken2** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3	**version**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d) IEC 62351-4:2018/AMD1:2020, 13.3.2 a)	m
4	**assoID**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) IEC 62351-4:2018/AMD1:2020, 13.3.2 b)	m
5	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the current local time value plus/minus 5 minutes.	IEC 62351-4:2018/AMD1:2020, 13.3.2 c) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
6	**seq**	If it the first data transfer by the client after the handshake exchange, check that this component has the value '0'. Otherwise, check that value is '1'1 greater than in the previous value.	IEC 62351-4:2018/AMD1:2020, 13.3.2 d)	m
7	**iv**	Shall be absent	IEC 62351-4:2018/AMD1:2020, 13.3.2 e)	m
8	**rekey**	When present, check the validity of the Diffie-Hellman public key with respect to the selected group.	IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	c1
9	**applData**	This component shall hold a valid unencrypted PrPDU provided by the protected protocol	IEC 62351-4:2018/AMD1:2020, 13.2.2 a.2)	m
10	**auth**	This component shall be checked for presence.	IEC 62351-4:2018/AMD1:2020, 13.2.2 b)	m

No	Component	Definition	Reference	Required
			IEC 62351-4:2018/AMD1:2020, 13.4.2	
11	**nonce**	If the ICV algorithm, species the presence of dynamic parameters, this component shall be present with the appropriate value, e.g., nonce.	IEC 62351-4:2018/AMD1:2020, 13.4.2 a)	m
12	**algo**	Check that the ICV algorithm specified is the same as the one specified the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.4.2 b)	m
13	**icv**	The ICV shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.4.2 c) IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.2.3	m
c1: The **applData** component shall be absent if the exception condition detected by the protected protocol should cause an alarm. Otherwise, it shall be present with the appropriate diagnostic information.				

Table 63 – Server initiated clear data transfer

No	Component	Definition	Reference	Required
1	**tbp**	Tbs includes part of the SecPDU that shall be protected by the ICV	IEC 62351-4:2018/AMD1:2020, 13.2.2 a)	m
2	**token2**	Shall hold the **ClearToken2** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3	**version**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d) IEC 62351-4:2018/AMD1:2020, 13.3.2 a)	m
4	**assoID**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) IEC 62351-4:2018/AMD1:2020, 13.3.2 b)	m
5	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the current local time value plus/minus 5 minutes.	IEC 62351-4:2018/AMD1:2020, 13.3.2 c) IEC 62351-4:2018/AMD1:2020, 13.1.2.	m
6	**seq**	If it the first data transfer by the server after the handshake exchange check that this component has the value '0'. Otherwise, check that value is '1' greater than in the previous value.	IEC 62351-4:2018/AMD1:2020, 13.3.2 d)	m
7	**iv**	Shall be absent	IEC 62351-4:2018/AMD1:2020, 13.3.2 e)	m
8	**reqRekey**	Check whether this component is present with the value **FALSE** or **TRUE** or whether it is absent	IEC 62351-4:2018/AMD1:2020, 13.3.2 g)	c1
9	**....changedKey**	Check whether this component is present with the value **FALSE** or **TRUE** or whether it is absent	IEC 62351-4:2018/AMD1:2020, 13.3.2 h)	c2
10	**applData**	This component shall hold a valid unencrypted PrPDU provided by the protected protocol	IEC 62351-4:2018/AMD1:2020, 13.2.2 a.2)	m

No	Component	Definition	Reference	Required
11	**auth**	This component shall be checked for presence.	IEC 62351-4:2018/AMD1:2020, 13.2.2 b) IEC 62351-4:2018/AMD1:2020, 13.4.2	m
12	**nonce**	If the ICV algorithm, species the presence of dynamic parameters, this component shall be present with the appropriate value, e.g., nonce.	IEC 62351-4:2018/AMD1:2020, 13.4.2 a)	m
13	**algo**	Check that the ICV algorithm specified is the same as the one specified the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 i) IEC 62351-4:2018/AMD1:2020, 13.4.2 b)	m
14	**icv**	The ICV shall be verified.	IEC 62351-4:2018/AMD1:2020, 13.4.2 c) IEC 62351-4:2018/AMD1:2020, 13.2.2 IEC 62351-4:2018/AMD1:2020, 13.2.3	m
c1: The **reqRekey** component shall be present with the value **TRUE** if the server or the client wants to initiate a key renewal process. Otherwise, it shall be absent or have the value **FALSE**. c2: The **changedKey** component shall be present with the value **TRUE** when the server informs the client that it is ready use a new set of symmetric keys. Otherwise, it shall be absent or have the value **FALSE**.				

9.9 E2E Encrypted data transfer subclass

This subclass is invoked when an encrypted data transfer PrPDU has been created. The input consists of:

- the PrPDU to be transmitted;
- if authenticated encryption is not used, the algorithm used for ICV generation;
- the encryption algorithm to be used;
- if transmitted by the client, whether it is time for renewal of symmetric keys;
- if transmitted by the server, whether changed key indication should be sent; and

- if transmitted by the server, whether a re-key request indication shall be sent.

Table 64 – Client initiated encrypted data transfer

No	Component	Definition	Reference	Required
1	**tbs**	Tbs includes part of the PDU that shall be protected by the digital signature.	IEC 62351-4:2018/AMD1:2020, 13.2.3	m
2	**token2**	Shall hold the **ClearToken2** components as specified below.	IEC 62351-4:2018/AMD1:2020, 13.3.2	m
3	**version**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 d) IEC 62351-4:2018/AMD1:2020, 13.3.2 a)	m
4	**assoID**	Check that it has the same value as in the corresponding **HandshakeAcc** SecPDU.	IEC 62351-4:2018/AMD1:2020, 13.3.1.1 e) IEC 62351-4:2018/AMD1:2020, 13.3.2 b)	m
5	**time**	Check that the syntax of the time value is in accordance with 13.1.2 of IEC 62351-4:2018/AMD1:2020, and if so, check that the time value is consistent with the current local time value plus/minus 5 minutes.	IEC 62351-4:2018/AMD1:2020, 13.3.2 c) IEC 62351-4:2018/AMD1:2020, 13.1.2..	m
6	**iv**	Shall be present if the symmetric key algorithm used for encryption requires dynamic parameters. Otherwise, it shall be absent,	IEC 62351-4:2018/AMD1:2020, 13.3.2 e)	m
7	**rekey**	When present, check the validity of the Diffie-Hellman public key with respect to the selected group.	IEC 62351-4:2018/AMD1:2020, 13.3.2 f)	c1
8	**applData**	This component shall hold an encrypted PrPDU provided by the protected protocol	IEC 62351-4:2018/AMD1:2020, 13.2.2 a.1)	m
9	**auth**	This component shall be checked for presence.	IEC 62351-4:2018/AMD1:2020, 13.2.3 b) IEC 62351-4:2018/AMD1:2020, 13.4.2	m
10	**nonce**	If the ICV algorithm, species the presence of dynamic parameters, this component shall be present with the appropriate value, e.g., nonce.	IEC 62351-4:2018/AMD1:2020, 13.4.2 a)	m