IEC TS 62351-100-3

Edition 1.0   2020-01

TECHNICAL
SPECIFICATION

colour
inside

Power systems management and associated information exchange – Data and communications security –
Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

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 It also gives information on projects, replaced and withdrawn publications.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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

IEC TS 62351-100-3

Edition 1.0 2020-01

TECHNICAL SPECIFICATION

colour inside

**Power systems management and associated information exchange – Data and communications security –
Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or

- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

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

IEC TS 62351-100-3, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/2090/DTS	57/2130/RVDTS

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

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

This document is to be read in conjunction with IEC 62351-3:2014, IEC 62351-3/AMD1:2018 and IEC 62351-3/AMD2:2020.

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

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

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

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

INTRODUCTION

This technical specification describes test cases for conformance testing of telecontrol equipment or systems integrating the IEC 62351-3 security extension for profiles including TCP/IP.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

1 Scope

This part of IEC 62351, which is a technical specification, describes test cases of data and communication security for telecontrol equipment, Substation Automation Systems [SAS] and telecontrol systems, including front-end functions of SCADA.

The goal of this document is to enable interoperability by providing a standard method of testing protocol implementations to verify that a device fulfils the requirement of IEC 62351-3. Note that conformity to IEC 62351-3 does not guarantee interoperability between devices using different implementations. It is expected that using this specification during testing will minimize the risk of non-interoperability. A basic condition for this interoperability is a passed conformance test of both devices.

The scope of this document is the specification of common available procedures and definitions for conformance and/or interoperability testing to ensure conformity to IEC 62351-3. The conformance test cases defined here are focused to verify the conformant integration of the underlying authentication/encryption protocol (TLS), as specified in IEC 62351-3, to protect TCP/IP based communications.

This document is not intended to test the underlying authentication/encryption protocol required by IEC 62351-3 to be implemented over TCP/IP (TLS). The conformance testing of the authentication/encryption protocol over TCP/IP is outside the scope of this document.

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.[1]

IEC TS 62351-2:2008, *Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles*

_____

[1] The base standard always takes precedence. In case of ambiguity between this technical specification and the base standards (IEC 62351-3), this part of IEC 62351 needs to be clarified or amended.

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

including TCP/IP
IEC 62351-3:2014/AMD1:2018, IEC 62351-3:2014/AMD2:2019

3   Terms, definitions and abbreviated terms

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

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

• IEC Electropedia: available at http://www.electropedia.org/

• ISO Online browsing platform: available at http://www.iso.org/obp

3.1   Terms and definitions

3.1.1
client
device receiving or requesting services or information from server devices

Note 1 to entry: In some specifications, a device is commonly called "controlling station" or "master" or "master station".

3.1.2
interoperability
ability of two or more telecontrol devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation

3.1.3
Message Authentication Code (MAC)
calculated value used by a receiving station to authenticate and check the integrity of an information

3.1.4
normal procedure tests
set of test cases to verify that the device fulfils the requirements of IEC 62351-3 in the expected (normal) conditions

3.1.5
Protocol Implementation Conformance Statement (PICS)
summary of the referencing standard capabilities of the system to be tested

3.1.6
Protocol Implementation Document (PID)
document which describes complete functionalities and system specific information

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

3.1.7
protocol Implementation eXtra Information for Testing (PIXIT)
system specific information contained in the PIXIT document regarding the capabilities of the system to be tested, which specifies which items are optional

3.1.8
resiliency tests
set of test cases to verify that the device fulfils the requirements of IEC 62351-3 in reacting to the unexpected (error) conditions

3.1.9
server
device that provides information or services to client devices

Note 1 to entry: In some specifications, a server is commonly called "controlled station" or "outstation" or "slave".

3.1.10
test equipment
all tools and instruments which simulate and verify the communication traffic, inputs and/or outputs of the system under test

3.1.11
test initiator
party initiating a conformance test of a device that is executed by a test facility

3.1.12
test facility
supplier-independent organization which is able to provide appropriate test equipment and trained staff for conformance testing

3.2   Abbreviated terms

Refer to IEC 62351-2 for a list of applicable abbreviated terms. The abbreviations listed below are included here because they are specific to IEC 62351-3 and they may be useful for reading this document as an independent document.

CRL   Certificate Revocation List

DUT   Device Under Test

IP   Inter-Networking Protocol

MAC   Message Authentication Code

OCSP   Online Certificate Status Protocol

PICS   Protocol Implementation Conformance Statement

PID   Protocol Implementation Document (=PICS + PIXIT)

PIXIT   Protocol Implementation eXtra Information for Testing

SAS   Substation Automation System

SCADA   Supervisory Control And Data Acquisition

TCP   Transport Control Protocol

4   General

4.1   Normatives covered by this document

This document defines the conformance test cases for the requirements defined in IEC 62351-3:2014, IEC 62351-3:2014/AMD1:2018, IEC 62351-3:2014/AMD2:2019 and the parts of the series requiring conformance to IEC 62351-3.

In addition to the test cases described in this document there are further test cases necessary for TLS base protocol RFC as well as test cases depending on the content provided in the certificates. An example may be the RBAC extension specified in IEC 62351-8 or certificate profiles defined in IEC 62351-9.

4.2   Conformance testing structure

4.2.1   General

IEC 62351-3 defines the requirements related to the authentication/encryption protocol, procedures and methods to be implemented at TCP/IP (transport) level.

The conformance test cases are divided into three clauses:

- Clause 5: Verification of configuration parameters. This clause contains the parameters specified by the standards referencing IEC 62351-3 (see IEC 62351-3:2014/AMD1:2018, Clause 7) and affecting the protocol behavior.

- Clause 6: Verification of IEC 62351-3 requirements. The goal of this clause is to verify that DUT is conformant to the requirements of the IEC 62351-3.

- Clause 7: Test result chart. This clause contains the results of the test cases listed in Clause 6 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. They are numbered, their numbering syntax is: Subclause number (where the table is located) + test case number.

In the column 'Reference' each test case has a direct reference to IEC 62351-3 where the clause under test is defined. PICS or PIXIT could be found in the "Reference" column for some test cases whenever the execution of the test case shall take into account specific parameter values declared in the PICS or PIXIT of the DUT.

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

M   =   Mandatory test case. The test is referencing to a clause that is mandatory in IEC 62351-3.

PICS

or

PIXIT =   Mandatory test case if the functionality is enabled in the PICS or PIXIT by marking the applicable check box or declaring the applicable value.

4.2.2   Conformance testing addressed per station type

The test cases in Clause 6 to verify the requirements defined in IEC 62351-3 are addressed per station type (client and server).

4.2.3   Normal procedure tests and resiliency tests

IEC 62351-3 specifies how each station (client and server) shall execute the procedures in normal conditions (expected behavior) and also how it shall behave when unexpected or fault events occur during their execution (negative behaviors). So, for each procedure in Clause 6 the test cases are also divided in two sections: the normal procedures test cases addressing the expected behaviors and the resiliency test cases addressing unexpected or fault events.

Normal Procedure tests and Resiliency tests shall be performed according to the parameters values supported by the DUT as defined in Clause 6, declared in the PICS and in the PIXIT of the DUT.

All the tests defined in this technical specification shall be executed for client stations and server stations unless otherwise specified in the test cases.

4.3   Conformance testing requirements

4.3.1   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 62351-3 shall execute an application protocol defined in a standard requiring conformance to IEC 62351-3.

4.3.2   Requirements for the device under test

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

a) The device ready for testing;

b) The Protocol Implementation Document (PID);

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

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

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

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

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

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

4.3.3   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 Clauses 5 and 6 shall be performed with no errors detected during testing.

* The test cases in Clause 6 should be performed in the order listed and the steps in each test case shall be followed, which means that the DUT is able to function as described in the specific test case.

* For each test case listed in Clauses 5 and 6 the test results need to be marked in the appropriate column of the test result chart in Clause 7. Each test case can either pass (Passed), or fail (Failed), or be not applicable (NA) when the configuration value is not supported by the device, or the test case cannot be performed (Empty). Ideally, there should be no empty boxes when the conformance testing is completed.

* Release a conformance test report of the DUT to the test initiator.

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