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.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 9
2 Normative references 9
3 Terms, definitions, and abbreviated terms 10
3.1 Terms and definitions 10
3.2 Abbreviated terms 11
4 Application structure and information flow 11
4.1 Overview 11
4.2 Application entity structure 12
4.3 Relationship to test structure 13
5 General 14
5.1 General guidelines 14
5.2 Test methodology 14
5.2.1 General 14
5.2.2 Normal procedure tests and resiliency tests 14
5.2.3 SubClass descriptions 14
5.3 Conformance testing requirements 15
5.3.1 Testing within the context of an application 15
5.3.2 Requirements for the device under test 15
5.3.3 Requirements for the test facility 15
5.3.4 Test Validation 16
5.4 PICS 16
5.5 PIXIT 17
5.6 Tests cases 18
6 E2E conformity testing in an OSI environment 22
6.1 Conformance tables for E2E OSI-security profile 22
6.2 E2E Test Procedures for OSI environment 25
6.2.1 Association Management 25
6.2.2 Clear Data Transfer 29
6.2.3 Encrypted Data Transfer 31
6.2.4 Rekey 34
7 E2E conformity testing in the XMPP environment 38
7.1 Conformance tables for E2E-XMPP security profile 38
7.2 E2E Test Procedures for XMPP environment 41
7.2.1 Association Management 41
7.2.2 Clear Data Transfer 44
7.2.3 Encrypted Data Transfer 45
7.2.4 Rekey 46
8 E2E Resiliency test procedures 49
8.1 General 49
8.2 Association Management Resiliency Testing 50
8.3 Clear Data Transfer Resiliency 59
8.4 Encrypted Data Transfer Resiliency 64
9 E2E security subclass (SecPDU) 68
9.1 E2E Handshake request subclass 68

9.2 E2E handshake accept subclass 71
9.3 E2E Application reject subclass 74
9.4 E2E Handshake reject subclass 76
9.5 E2E Handshake security abort subclass 78
9.6 E2E Data transfer security abort subclass 80
9.7 E2E Abort by protected protocol subclass 82
9.8 E2E Clear data transfer subclass 84
9.9 E2E Encrypted data transfer subclass 88
9.10 E2E Association release request subclass 92
9.11 E2E Association release response subclass 94
10 OSI subclass (EnvPDU) 96
10.1 OSI association request subclass 96
10.2 OSI association response subclass 98
10.3 OSI abort subclass 100
10.4 OSI clear data transfer subclass 103
10.5 OSI encrypted data transfer subclass 103
10.6 OSI release request subclass 104
10.7 OSI release response subclass 104
11 XMPP subclass (EnvPDU) 105
11.1 XMPP IQ stanza subclass 105
11.2 XMPP message stanza subclass 108
11.3 XMPP error subclass 109

Figure 1 – Application entity structure and information flow 12
Figure 2 – Relationships between APDUs 12
Figure 3 – Structure for test specifications 13

Table 1 – PIXIT for Base Profile 17
Table 2 – PIXIT for Secure Communication 18
Table 3 – IEC 62351-4:2018/AMD1:2020 E2E Compliancy Testing (IEC 61850-8-1 and ICCP) 19
Table 4 – IEC 62351-4:2018/AMD1:2020 E2E Compliancy Testing (IEC 61850-8-2) 21
Table 5 – Base Profile – E2E Security 23
Table 6 – Protocol Handshake – E2E Security 23
Table 7 – IEC 61850 Application Association – E2E Security 23
Table 8 – OSI EnvPDU Supported – E2E Security 23
Table 9 – OSI EnvPDU Subclass Supported – E2E Security 23
Table 10 – E2E SecPDU Subclass Supported 24
Table 11 – OSI Mode of encryption – E2E Security 24
Table 12 – Cryptographic algorithms – E2E Security 24
Table 13 – ASN.1 Objects – E2E Security 25
Table 14 – Verification of Client handshake request procedure in OSI environment 26
Table 15 – Verification of Server handshake request procedure in OSI environment 27
Table 16 – Handshake request resiliency procedure in OSI environment – Client 28
Table 17 – Handshake request resiliency procedure in OSI environment – Server 29

Table 18 – Verification of requirements for OSI environment security – Clear Data transfer 30
Table 19 – Clear Data Transfer resiliency procedure in OSI environment – Client 30
Table 20 – Clear Data Transfer resiliency procedure in OSI environment – Server 31
Table 21 – Verification of requirements for OSI environment security – Encrypted data transfer 32
Table 22 – Resiliency testing for client – Encrypted data transfer 33
Table 23 – Resiliency testing for server – Encrypted data transfer 34
Table 24 – Verification of requirements for OSI environment security – Rekey initiated by the client 35
Table 25 – Verification of requirements for OSI environment security – Rekey initiated by the Server 36
Table 26 – Base Profile – E2E XMPP Security 38
Table 27 – Protocol Handshake – E2E XMPP Security 38
Table 28 – IEC 61850 Application Association – E2E XMPP Security 38
Table 29 – EnvPDU Parameters– E2E XMPP Security 39
Table 30 – EnvPDU Supported– E2E XMPP Security 39
Table 31 – SecPDU Subclasses– E2E XMPP Security 39
Table 32 – Encryption – E2E XMPP Security 40
Table 33 – Cryptographic algorithms – E2E XMPP Security 40
Table 34 – XMPP – E2E XMPP Security 40
Table 35 – XMPP– E2E XMPP Security 41
Table 36 – XMPP T-profile – E2E XMPP Security 41
Table 37 – Verification of client handshake request procedure in XMPP environment 42
Table 38 – Verification of server handshake request procedure in XMPP environment 43
Table 39 – Handshake request resiliency procedure in XMPP environment – Client 43
Table 40 – Handshake request resiliency procedure in XMPP environment – Server 44
Table 41 – Verification of requirements for XMPP environment security – Clear Data transfer 44
Table 42 – Clear Data Transfer resiliency procedure in XMPP environment – Server 45
Table 43 – Clear Data Transfer resiliency procedure in XMPP environment – Client 45
Table 44 – Verification of requirements for XMPP environment security – Encrypted data transfer 45
Table 45 – Resiliency testing for client – Encrypted data transfer 46
Table 46 – Resiliency testing for server – Encrypted data transfer 46
Table 47 – Verification of requirements for XMPP environment security – Rekey initiated by the client 47
Table 48 – Verification of requirements for XMPP environment security – Rekey initiated by the server 48
Table 49 – Handshake request resiliency procedure – Client 50
Table 50 – Handshake request resiliency procedure – Server 55
Table 51 – Clear Data Transfer resiliency – Server 59
Table 52 – Clear Data Transfer resiliency – Client 61
Table 53 – Resiliency testing for client – Encrypted data transfer 64
Table 54 – Resiliency testing for server – Encrypted data transfer 66
Table 55 – E2E handshake request subclass 69

Table 56 – E2E handshake accept subclass. 71
Table 57 – E2E Application reject subclass 75
Table 58 – Server reject of association due to security issues 77
Table 59 – Test of client submitted handshake security abort 79
Table 60 – Client or server emitted data transfer security abort 81
Table 61 – Client or server emitted abort by protected protocol 83
Table 62 – Client initiated clear data transfer 85
Table 63 – Server initiated clear data transfer 87
Table 64 – Client initiated encrypted data transfer 89
Table 65 – Server initiated encrypted data transfer 91
Table 66 – Client or server issued association release request. 93
Table 67 – Client or server association release response 95
Table 68 – OSI association request subclass 97
Table 69 – OSI association response subclass 99
Table 70 – Client OSI abort subclass 101
Table 71 – Server OSI abort subclass 102
Table 72 – Client or server OSI environment clear data transfer 103
Table 73 – Client or server OSI environment encrypted data transfer 103
Table 74 – OSI release request subclass 104
Table 75 – OSI release response subclass 105
Table 76 – Client XMPP iq stanza subclass 106
Table 77 – Server XMPP IQ stanza subclass 107
Table 78 – Client XMPP message stanza subclass 108
Table 79 – Server XMPP message stanza subclass 109

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*