



BSI Standards Publication

Power systems management and associated information exchange - Data and communications security

Part 3: Communication network and system security - Profiles including TCP/IP

National foreword

This British Standard is the UK implementation of EN 62351-3:2014+A2:2020. It is identical to IEC 62351-3:2014, incorporating amendments 1:2018 and 2:2020. It supersedes BS EN 62351-3:2014+A1:2018, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by **A1** **A1**.

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

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

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

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 03482 0

ICS 33.200

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2015.

Amendments/corrigenda issued since publication

Date	Text affected
31 October 2018	Implementation of IEC amendment 1:2018 with CENELEC endorsement A1:2018
31 May 2020	Implementation of IEC amendment 2:2020 with CENELEC endorsement A2:2020

English Version

**Power systems management and associated information
exchange - Data and communications security - Part 3:
Communication network and system security - Profiles including
TCP/IP
(IEC 62351-3:2014)**

Gestion des systèmes de puissance et échanges
d'informations associés - Sécurité des communications et
des données - Partie 3: Sécurité des réseaux et des
systèmes de communication - Profils comprenant TCP/IP
(IEC 62351-3:2014)

Management von Systemen der Energietechnik und
zugehöriger Datenaustausch - Daten- und
Kommunikationssicherheit - Teil 3: Sicherheit von
Kommunikationsnetzen und Systemen - Profile
einschließlich TCP/IP
(IEC 62351-3:2014)

This European Standard was approved by CENELEC on 2014-12-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 57/1498/FDIS, future edition 1 of IEC 62351-3, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-3:2014.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2015-09-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2017-12-02

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62351-3:2014 was approved by CENELEC as a European Standard without any modification.

Foreword to amendment A1

The text of document 57/1976/FDIS, future edition 1 of IEC 62351-3/A1, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-3:2014/A1:2018.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2019-03-29
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-06-29

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62351-3:2014/A1:2018 was approved by CENELEC as a European Standard without any modification.

Foreword to amendment A2

The text of document 57/2149/FDIS, future IEC 62351-3/A2, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-3:2014/A2:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-01-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-04-02

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62351-3:2014/A2:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62351-7	NOTE	Harmonized as EN 62351-7
IEC 62351-14 ¹	NOTE	Harmonized as EN IEC 62351-14 ²

¹ To be published. Stage at the time of publication: IEC/PCC 62351-14:2020.

² To be published. Stage at the time of publication: prEN IEC 62351-14:2019.

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TS 62351-1	2007	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	-	-
IEC/TS 62351-2	2008	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
IEC 62351-7	-	Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models	EN 62351-7	-
IEC 62351-9	-	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment	EN 62351-9	-
ISO/IEC 9594-8	2017	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
RFC 4492	2006	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	-	-
RFC 5246	2008	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
RFC 5280	2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-
RFC 5746	2010	Transport Layer Security (TLS) Renegotiation Indication Extension	-	-
RFC 6066	2006	Transport Layer Security (TLS) Extensions: Extension Definitions	-	-
RFC 6176	2011	Prohibiting Secure Sockets Layer (SSL) Version 2.0	-	-

CONTENTS

FOREWORD	3
INTRODUCTION to Amendment 2	5
1 Scope	6
1.1 Scope	6
1.2 Intended Audience	6
2 Normative references	6
3 Terms, definitions and abbreviations	7
3.1 Terms, definitions and abbreviations	7
3.2 Additional abbreviations	7
4 Security issues addressed by this standard	7
4.1 Operational requirements affecting the use of TLS in the telecontrol environment	7
4.2 Security threats countered	8
4.3 Attack methods countered	8
4.4 Handling of security events	8
5 Mandatory requirements	9
5.1 Deprecation of cipher suites	9
5.2 Negotiation of versions	9
5.3 Session resumption	10
5.4 Session renegotiation	11
5.5 Message Authentication Code	12
5.6 Certificate support	12
5.7 Co-existence with non-secure protocol traffic	16
6 Optional security measure support	16
7 Referencing standard requirements	16
8 Conformance	17
8.1 General	17
8.2 Notation	17
8.3 Conformance to selected cipher suites	17
8.4 Conformance to selected TLS versions	17
8.5 Conformance to selected TLS protocol features	17
8.6 Conformance to certificate support	18
8.7 Conformance to cryptographic algorithm support	18
Bibliography	20
 Table 1 – Conformance to TLS cipher suites	 17
Table 2 – Conformance to TLS versions	17
Table 3 – Conformance to TLS protocol features	18
Table 4 – Conformance to certificate support	18
Table 5 – Conformance to cryptographic algorithm support	19

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 3: Communication network and system security – 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.

International Standard IEC 62351-3 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This standard cancels and replaces IEC TS 62351-3:2007.

The text of this standard is based on the following documents:

FDIS	Report on voting
57/1498/FDIS	57/1515/RVD

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