ICS 33.200 SLOVENSKÁ TECHNICKÁ NORMA Október 2023

STN	**Riadenie elektrických výkonových sústav a pridružená výmena informácií Bezpečnosť údajov a komunikácií Časť 3: Bezpečnosť komunikačných sietí a systémov Profily vrátane TCP/IP**	**STN EN IEC 62351-3** 33 4622

Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 09/23

Obsahuje: EN IEC 62351-3:2023, IEC 62351-3:2023

Oznámením tejto normy sa od 11.07.2026 ruší
STN EN 62351-3 (33 4622) z augusta 2015

obsahuje farebné strany

137517

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62351-3

July 2023

ICS 33.200

Supersedes EN 62351-3:2014; EN 62351-3:2014/A1:2018; EN 62351-3:2014/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 62351-3:2023)

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 62351-3:2023)

Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen - Daten- und Kommunikationssicherheit - Teil 3: Sicherheit von Kommunikationsnetzen und Systemen - Profile einschließlich TCP/IP
(IEC 62351-3:2023)

This European Standard was approved by CENELEC on 2023-07-11. 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye 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 57/2578/FDIS, future edition 2 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 IEC 62351-3:2023.

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) 2024-04-11
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2026-07-11

This document supersedes EN 62351-3:2014 and all of its amendments and corrigenda (if any).

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 Standardization Request given to CENELEC by the European Commission and the European Free Trade Association.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62351-3:2023 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 standard indicated:

IEC 62351-4:2018	NOTE	Approved as EN IEC 62351-4:2018 (not modified)
IEC 62351-4:2018/A1:2020	NOTE	Approved as EN IEC 62351-4:2018/A1:2020 (not modified)
IEC 62351-5	NOTE	Approved as EN IEC 62351-5
IEC 62351-6:2020	NOTE	Approved as EN IEC 62351-6:2020 (not modified)
IEC 62351-7	NOTE	Approved as EN 62351-7
IEC 62351-8:2020	NOTE	Approved as EN IEC 62351-8:2020 (not modified)

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.cencenelec.eu.

Publication	Year	Title	EN/HD	Year
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 62351-9	-	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment	-	-
ISO/IEC 9594-8	2020	Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks	-	-
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 5288	2008	AES Galois Counter Mode (GCM) Cipher Suites for TLS	-	-
RFC 5289	2008	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	-	-
RFC 5746	2010	Transport Layer Security (TLS) Renegotiation Indication Extension	-	-
RFC 6066	2011	Transport Layer Security (TLS) Extensions: Extension Definitions	-	-
RFC 6176	2011	Prohibiting Secure Sockets Layer (SSL) Version 2.0	-	-
RFC 8422	2018	ECC Cipher Suites for TLSv1.2 and earlier	-	-
RFC 8446	2018	The TLS Protocol Version 1.3	-	-
RFC 9150	2021	TLS 1.3 Authentication and Integrity only Cipher Suites	-	-

IEC 62351-3

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

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 62351-3:2023-06(en-fr)

IEC 62351-3

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200 ISBN 978-2-8322-6935-0

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
1.1 Scope 8
1.2 Intended audience 8
2 Normative references 9
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 10
4 Security issues addressed by this document 10
4.1 General 10
4.2 Security threats countered 11
4.3 Attack methods countered 11
4.4 Handling of security events 12
5 Overview of differences in TLS versions 12
5.1 General 12
5.2 Main differences between TLSv1.2 and TLSv1.3 12
5.3 Cipher suite naming 13
5.4 Backward compatibility 14
5.5 Extensions 14
6 Generic requirements 15
6.1 General 15
6.2 Signalling of supported TLS versions 15
6.3 Usage of non-encrypting cipher suites 16
6.4 Certificate support 17
6.4.1 Support of multiple trust anchors 17
6.4.2 Certificate size 17
6.4.3 Certificate exchange 17
6.4.4 Public-key certificate validation 18
6.5 Co-existence with non-secure protocol traffic 21
7 Requirements specific to TLSv1.2 21
7.1 General 21
7.2 Supported cipher suites 21
7.3 Disallowed cipher suites 22
7.4 Key exchange 22
7.4.1 General 22
7.4.2 Key exchange mechanisms 22
7.4.3 Cryptographic algorithms 22
7.4.4 Session resumption 24
7.4.5 Session renegotiation 25
7.5 Support of extensions 26
7.5.1 General 26
7.5.2 TLS session renegotiation extension 26
7.5.3 Signalling of client supported CA certificates via Trusted CA 27
7.5.4 Signalling of supported signature algorithms 27
7.5.5 Stapling of OCSP response messages 28

7.5.6 Signalling of intended target TLS server via Server Name Indication 29
7.5.7 Support of encryption before authentication 29
8 Requirements specific to TLSv1.3 30
8.1 General 30
8.2 Supported cipher suites 30
8.3 Key exchange 30
8.3.1 General 30
8.3.2 Handshake modes 31
8.3.3 Diffie-Hellman Groups 32
8.3.4 Signature algorithms 32
8.4 Session key update (post-handshake message) 33
8.5 New session ticket (post-handshake message) 34
8.6 Session resumption 34
8.7 Certificate validation 34
8.8 Support of extensions 35
8.8.1 General 35
8.8.2 Signalling of supported TLS versions 35
8.8.3 Cookie 35
8.8.4 Signalling of supported signature algorithms 35
8.8.5 Signalling of supported groups 36
8.8.6 Signalling of key share 36
8.8.7 Signalling of intended target TLS server via Server Name Indication 36
8.8.8 Signalling of supported certificate authorities 37
8.8.9 Support of PSK based key agreement 37
8.8.10 Stapling of OCSP response messages 37
8.8.11 Signalling of early data 38
9 Optional security measure support 38
10 Conformance 38
10.1 General 38
10.2 Notation 38
10.3 Conformance to selected TLS versions 38
10.4 Conformance to certificate handling 39
10.5 Conformance to TLSv1.2 specifics 39
10.5.1 Conformance to selected cipher suites 39
10.5.2 Conformance to cryptographic algorithm support 40
10.5.3 Conformance to TLSv1.2 session management features 40
10.5.4 Conformance to selected TLSv1.2 extensions 41
10.6 Conformance to TLSv1.3 specifics 41
10.6.1 Conformance to selected TLSv1.3 cipher suites 41
10.6.2 Conformance to selected TLSv1.3 session management features 42
10.6.3 Conformance to selected TLSv1.3 extensions 44
10.6.4 Conformance to selected TLSv1.3 post-handshake messages 44
Annex A (informative) Security Events 46
A.1 Security event logs 46
A.2 Mapping of TLS events related to the TLS handshake 46
A.3 Mapping of TLS events related to the certificate handling 48
Bibliography 49

Figure 1 – Definition of cipher suites according to TLSv1.2 (RFC 5246) 14
Figure 2 – Definition of cipher suites according to TLSv1.3 (RFC 8446) 14

Table 1 – Support of cipher suites for TLSv1.2 21
Table 2 – Support of cipher suites for TLSv1.3 30
Table 3 – Support of PSK-based handshake modes for TLSv1.3 31
Table 4 – Support of Diffie Hellman Groups for TLSv1.3 32
Table 5 – Supported signature algorithms for the handshake in TLSv1.3 32
Table 6 – Supported signature algorithms for the certificates in TLSv1.3 33
Table 7 – Conformance to TLS versions 38
Table 8 – Conformance to certificate support 39
Table 9 – Conformance to TLSv1.2 usable cipher suites 40
Table 10 – Conformance to cryptographic algorithm support 40
Table 11 – Conformance to TLSv1.2 session management features 41
Table 12 – Conformance to TLSv1.2 handshake extensions 41
Table 13 – Conformance to TLSv1.3 cipher suites 42
Table 14 – Conformance to handshake modes of TLSv1.3 42
Table 15 –Conformance to early data feature (0-RTT) of TLSv1.3 42
Table 16 – Conformance to supported Diffie Hellman Groups in TLSv1.3 43
Table 17 – Conformance to supported signature algorithms for the handshake in TLSv1.3 43
Table 18 – Conformance to supported signature algorithms for the certificates in TLSv1.3 44
Table 19 – Conformance to TLSv1.3 extensions 44
Table 20 – Conformance to post-handshake messages of TLSv1.3 45
Table A.1 – Security event logs related to TLS handshake defined in IEC 62351-3:— (Ed.2) mapped to IEC 62351-14 46
Table A.2 – Security event logs related to certificate validation defined in IEC 62351-3 Ed.2 mapped to IEC 62351-14 48

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.

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

This second edition cancels and replaces the first edition published in 2014, Amendment 1:2018 and Amendment 2:2020. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Inclusion of the TLSv1.2 related parameter required in IEC 62351-3 Ed.1.2 to be specified by the referencing standard. This comprises the following parameter:
   - Mandatory TLSv1.2 cipher suites to be supported.
   - Specification of session resumption parameters.
   - Specification of session renegotiation parameters.

- Revocation handling using CRL and OCSP.
- Handling of security events.

b) Inclusion of a TLSv1.3 profile to be applicable for the power system domain in a similar way as for TLSv1.2 session.

The text of this International Standard is based on the following documents:

Draft	Report on voting
57/2578/FDIS	57/2593/RVD

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 International Standard is English.

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.

NOTE The following print types are used:

- Abstract Syntax Notation One (ASN.1) are presented in `courier new` and **`bold courier new`**

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 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

This edition of IEC 62351-3 is a self-contained document profiling the usage of TLS for to secure power system communication. It is recommended to refer to this edition of this document rather than any previous edition, because this edition updates the utilized cryptographic algorithms (ciphersuites), provides enhanced functionality, and covers different TLS versions. In contrast to previous editions, this document specifies all necessary TLS specific settings and does not require the referencing standard to define specific settings for TLS.

Note that the recommendation to use this edition, potentially also with older referencing standards, requires technical support by implementations of the TLS settings specified in this edition of the document.

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

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

1 Scope

1.1 Scope

This part of IEC 62351 specifies how to provide confidentiality, integrity protection, and message level authentication for protocols that make use of TCP/IP as a message transport layer and utilize Transport Layer Security when cyber-security is required. This may relate to SCADA/telecontrol, protection, automation and control protocols.

IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (TLSv1.2 defined in RFC 5246, TLSv1.3 defined in RFC 8446). In the specific clauses, there will be subclauses to note the differences and commonalities in the application depending on the target TLS version. The use and specification of intervening external security devices (e.g., "bump-in-the-wire") are considered out-of-scope.

In contrast to previous editions of this document, this edition is self-contained in terms of completely defining a profile of TLS. Hence, it can be applied directly, without the need to specify further TLS parameters, except the port number, over which the communication will be performed. Therefore, this part can be directly utilized from a referencing standard and can be combined with further security measures on other layers. Providing the profiling of TLS without the need for further specifying TLS parameters allows declaring conformity to the described functionality without the need to involve further IEC 62351 documents.

This document is intended to be referenced as a normative part of other IEC standards that have the need for providing security for their TCP/IP-based protocol exchanges under similar boundary conditions. However, it is up to the individual protocol security initiatives to decide if this document is to be referenced.

The document also defines security events for specific conditions, which support error handling, security audit trails, intrusion detection, and conformance testing. Any action of an organization in response to events to an error condition described in this document are beyond the scope of this document and are expected to be defined by the organization’s security policy.

This document reflects the security requirements of the IEC power systems management protocols. Should other standards bring forward new requirements, this document may need to be revised.

1.2 Intended audience

The initial audience for this document is intended to be experts developing or making use of protocols in the field of power systems management and associated information exchange. For the measures described in this document to take effect, they must be accepted and referenced by the specifications of protocols making use of TCP/IP security by applying TLS. This document is written to enable that process.

The subsequent audience for this document is intended to be the developers of products that implement these protocols.

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

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 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 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

RFC 5246:2008, *The TLS Protocol Version 1.2*[1]

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5288:2008, *AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289:2008, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension*

RFC 6066:2011, *Transport Layer Security Extensions*

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*

RFC 8422:2018, *ECC Cipher Suites for TLSv1.2 and earlier*

RFC 8446:2018, *The TLS Protocol Version 1.3*

RFC 9150:2021, *TLS 1.3 Authentication and Integrity only Cipher Suites*