ICS 33.200 SLOVENSKÁ TECHNICKÁ NORMA Október 2023

STN	**Riadenie elektrických výkonových sústav a pridružená výmena informácií Bezpečnosť údajov a komunikácií Časť 9: Manažérstvo kľúčov kybernetickej bezpečnosti pre zariadenia elektrických výkonových sústav**	**STN EN IEC 62351-9** 33 4622

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

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 62351-9:2023, IEC 62351-9:2023

Oznámením tejto normy sa od 11.07.2026 ruší
STN EN 62351-9 (33 4622) z decembra 2017

obsahuje farebné strany

137514

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62351-9

July 2023

ICS 33.200

Supersedes EN 62351-9:2017

English Version

Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9:2023)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance (IEC 62351-9:2023)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 9: Cyber security Schlüssel-Management für Stromversorgungsanlagen (IEC 62351-9:2023)

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

Ref. No. EN IEC 62351-9:2023 E

European foreword

The text of document 57/2579/FDIS, future edition 2 of IEC 62351-9, 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 62351-9:2023.

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 62351-9:2017 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 addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

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 62351-9:2023 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:

ISO/IEC 19790:2012	NOTE	Approved as EN ISO/IEC 19790:2020 (not modified)
IEC 62351-8	NOTE	Approved as EN IEC 62351-8
ISO/IEC 19790	NOTE	Approved as EN ISO/IEC 19790
IEC 62443-3-3	NOTE	Approved as EN IEC 62443-3-3
IEC 62443-4-2	NOTE	Approved as EN IEC 62443-4-2

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 62351-2	-	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
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	-	-
IEC 62351-4	-	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives	EN IEC 62351-4	-
IEC 62351-5	-	Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives	EN IEC 62351-5	-
IEC 62351-6	-	Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850	EN IEC 62351-6	-
IEC 62351-14	—[1]	Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging	-	-
ISO/IEC 9594-8	2020	Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks	-	-
ISO/IEC 9594-11	2020	Information technology - Open systems interconnection directory - Part 11: Protocol specifications for secure operations	-	-

[1] Under preparation. Stage at the time of publication: IEC/ACDV 62351-14:2023.

EN IEC 62351-9:2023 (E)

Publication	Year	Title	EN/HD	Year
ISO/IEC 9834-1	2012	Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree	-	-
IETF RFC 5272	-	Certificate Management over CMS (CMC)	-	-
IETF RFC 5755	-	An Internet Attribute Certificate Profile for Authorization	-	-
IETF RFC 5934	-	Trust Anchor Management Protocol (TAMP)	-	-
IETF RFC 6407	-	The Group Domain of Interpretation	-	-
IETF RFC 6960	-	X.509 - Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	-	-
IETF RFC 7030	-	Enrolment over Secure Transport	-	-
IETF RFC 8052	-	Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security	-	-
IETF RFC 8263	-	Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message	-	-
IETF RFC 8894	-	Simple Certificate Enrolment Protocol	-	-

IEC 62351-9

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance

IEC 62351-9:2023-06(en-fr)

IEC 62351-9

Edition 2.0 2023-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200 ISBN 978-2-8322-6950-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 9: Cyber security key management for power system equipment

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 62351-9 has been prepared by WG15: Data and Communication Security, of IEC technical committee TC57: Power systems management and associated information exchange. It is an International Standard.

This second edition cancels and replaces the first edition published in 2017. This edition constitutes a technical revision.

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

a) Certificate components and verification of the certificate components have been added;
b) GDOI has been updated to include findings from interop tests;
c) GDOI operation considerations have been added;
d) GDOI support for PTP (IEEE 1588) support has been added as specified by IEC/IEEE 61850-9-3 Power Profile;
e) Cyber security event logging has been added as well as the mapping to IEC 62351-14;

f) Annex B with background on utilized cryptographic algorithms and mechanisms has been added.

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

Draft	Report on voting
57/2579/FDIS	57/2594/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): `in courier new` and **`bold courier new`** `type`.

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.

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

Part 9: Cyber security key management for power system equipment

1 Scope

This part of IEC 62351 specifies cryptographic key management, primarily focused on the management of long-term keys, which are most often asymmetric key pairs, such as public-key certificates and corresponding private keys. As certificates build the base this document builds a foundation for many IEC 62351 services (see also Annex A). Symmetric key management is also considered but only with respect to session keys for group-based communication as applied in IEC 62351-6. The objective of this document is to define requirements and technologies to achieve interoperability of key management by specifying or limiting key management options to be used.

This document assumes that an organization (or group of organizations) has defined a security policy to select the type of keys and cryptographic algorithms that will be utilized, which may have to align with other standards or regulatory requirements. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. This document assumes that the reader has a basic understanding of cryptography and key management principles.

The requirements for the management of pairwise symmetric (session) keys in the context of communication protocols is specified in the parts of IEC 62351 utilizing or specifying pairwise communication such as:

- IEC 62351-3 for TLS by profiling the TLS options
- IEC 62351-4 for the application layer end-to-end security
- IEC TS 62351-5 for the application layer security mechanism for IEC 60870-5-101/104 and IEEE 1815 (DNP3)

The requirements for the management of symmetric group keys in the context of power system communication protocols is specified in IEC 62351-6 for utilizing group security to protect GOOSE and SV communication. IEC 62351-9 utilizes GDOI as already IETF specified group-based key management protocol to manage the group security parameter and enhances this protocol to carry the security parameter for GOOSE, SV, and PTP.

This document also defines security events for specific conditions which could identify issues which might require error handling. However, the actions of the organisation in response to these error conditions are beyond the scope of this document and are expected to be defined by the organizations security policy.

In the future, as public-key cryptography becomes endangered by the evolution of quantum computers, this document will also consider post-quantum cryptography to a certain extent. Note that at this time being no specific measures are provided.

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

IEC 62351-3:—[1], *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

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

IEC 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

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

IEC 62351-14:—[2], *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging*

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

ISO/IEC 9594-11:2020, Rec. ITU-T X.510 (2020), *Information technology – Open systems interconnection – The Directory: Protocol specifications for secure operations*

ISO/IEC 9834-1:2012, Rec. ITU-T X.660 (2011), *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*

IETF RFC 5272, *Certificate Management over CMS (CMC)*

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

IETF RFC 5934, *Trust Anchor Management Protocol (TAMP)*

IETF RFC 6407, *The Group Domain of Interpretation*

IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

IETF RFC 7030, *Enrolment over Secure Transport*

IETF RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security*

_____

[1] Under preparation. Stage at the time of publication: IEC/RFDIS 62351-3:2023.

[2] Under preparation. Stage at the time of publication: IEC/ACDV 62351-14:2023.

IETF RFC 8263, *Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message*

IETF RFC 8894, *Simple Certificate Enrolment Protocol*