ICS 33.200 SLOVENSKÁ TECHNICKÁ NORMA Máj 2023

| STN | **Riadenie elektrických výkonových sústav a pridružená výmena informácií Bezpečnosť údajov a komunikácií Časť 5: Bezpečnosť podľa IEC 60870-5 a deriváty** | **STN EN IEC 62351-5**<br><br>33 4622 |
|---|---|---|

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

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. 04/23

Obsahuje: EN IEC 62351-5:2023, IEC 62351-5:2023

obsahuje farebné strany

**136745**

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2023
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN IEC 62351-5

February 2023

ICS 33.200

English Version

# Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives (IEC 62351-5:2023)

Gestion des systèmes de puissance et échanges d'informations associées - Sécurité des communications et des données - Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés (IEC 62351-5:2023)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 5: Sicherheit für IEC 60870-5 und Derivate (IEC 62351-5:2023)

This European Standard was approved by CENELEC on 2023-02-17. 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**

© 2023 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62351-5:2023 E

**EN IEC 62351-5:2023 (E)**

# European foreword

The text of document 57/2516/FDIS, future edition 1 of IEC 62351-5, 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 62351-5:2023.

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) | 2023-08-17 |
| • latest date by which the national standards conflicting with the document have to be withdrawn | (dow) | 2026-02-17 |

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.

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 62351-5:2023 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 60870-5-101:2003 | NOTE Approved as EN 60870-5-101:2003 (not modified) |
| IEC 60870-5-102 | NOTE Approved as EN 60870-5-102 |
| IEC 60870-5-103 | NOTE Approved as EN 60870-5-103 |
| IEC 60870-5-104 | NOTE Approved as EN 60870-5-104 |

# Annex A
(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.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC 60870-5 | series | Telecontrol equipment and systems – Part 5: Transmission protocols | EN 60870-5 | series |
| IEC/TS 62351-1 | - | 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 | - | Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms | - | - |
| IEC 62351-3 | - | Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP | EN 62351-3 | - |
| 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 62351-8 | - | Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management | EN IEC 62351-8 | - |
| IEC 62351-14[1] | - | Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging | - | - |

[1] Under preparation. Stage at the time of publication: IEC ACDV 62351-14:2021.

**EN IEC 62351-5:2023 (E)**

| | | | | |
|---|---|---|---|---|
| IETF RFC 2104 | - | HMAC: Keyed-Hashing for Message Authentication | - | - |
| IETF RFC 3394 | - | Advanced Encryption Standard (AES) Key Wrap Algorithm | - | - |
| IETF RFC 5116 | - | An Interface and Algorithms for Authenticated Encryption | - | - |
| IETF RFC 5869 | - | HMAC-based Extract-and-Expand Key Derivation Function | - | - |
| IETF RFC 7693 | - | The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC) | - | - |
| IETF RFC 7748 | - | Elliptic Curves for Security | - | - |
| SEC2-V2 | - | Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain parameters - Version 2.0 | - | - |

# IEC 62351-5

Edition 1.0 2023-01

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

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

## Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

IEC 62351-5:2023-01 (en-fr)

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2023 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

**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.

**IEC Products & Services Portal - products.iec.ch**
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

---

**A propos de l'IEC**
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

**A propos des publications IEC**
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

**Recherche de publications IEC - webstore.iec.ch/advsearchform**
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

**IEC Just Published - webstore.iec.ch/justpublished**
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

**Service Clients - webstore.iec.ch/csc**
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

**IEC Products & Services Portal - products.iec.ch**
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

**Electropedia - www.electropedia.org**
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

# IEC 62351-5

Edition 1.0 2023-01

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

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

## Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-6017-3

**Warning! Make sure that you obtained this publication from an authorized distributor.**
**Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

# CONTENTS

FOREWORD ..... 6
1 Scope ..... 8
2 Normative references ..... 9
3 Terms and definitions ..... 10
4 Abbreviated terms ..... 11
5 Problem description ..... 12
5.1 Overview of clause ..... 12
5.2 Specific threats addressed ..... 12
5.3 Design issues ..... 12
5.3.1 Overview of subclause ..... 12
5.3.2 Asymmetric communications ..... 12
5.3.3 Message-oriented ..... 12
5.3.4 Poor sequence numbers or no sequence numbers ..... 13
5.3.5 Limited processing power ..... 13
5.3.6 Limited bandwidth ..... 13
5.3.7 No access to authentication server ..... 13
5.3.8 Limited frame length ..... 13
5.3.9 Limited checksum ..... 14
5.3.10 Radio systems ..... 14
5.3.11 Dial-up systems ..... 14
5.3.12 Variety of protocols affected ..... 14
5.3.13 Differing data link layers ..... 14
5.3.14 Long upgrade intervals ..... 15
5.3.15 Remote sites ..... 15
5.3.16 Unreliable media ..... 15
5.4 General principles ..... 15
5.4.1 Overview of subclause ..... 15
5.4.2 Application layer only ..... 15
5.4.3 Generic definition mapped onto different protocols ..... 15
5.4.4 Bi-directional ..... 15
5.4.5 Management of cryptographic keys ..... 15
5.4.6 Backwards tolerance ..... 16
5.4.7 Upgradeable ..... 16
5.4.8 Multiple connections ..... 16
6 Theory of operation ..... 16
6.1 Overview of clause ..... 16
6.2 The secure communication ..... 16
6.2.1 Basic concepts ..... 16
6.2.2 Association ID ..... 17
6.2.3 Authenticating ..... 18
6.2.4 Central Authority ..... 18
6.2.5 Role Based Access Control (RBAC) ..... 18
6.2.6 Cryptographic keys ..... 18
6.2.7 Security statistics ..... 22
6.2.8 Security events ..... 22
7 Functional requirements ..... 22

7.1 Overview of clause ..... 22
7.2 Procedures Overview ..... 22
7.3 State machine overview ..... 23
7.4 Timers and counters ..... 25
7.5 Security statistics and events ..... 25
7.5.1 General ..... 25
7.5.2 Special security thresholds ..... 29
7.5.3 Security statistics reporting ..... 29
7.5.4 Security events monitoring and logging ..... 29
8 Formal procedures ..... 30
8.1 Overview of subclause ..... 30
8.2 Distinction between messages and ASDUs ..... 30
8.2.1 General ..... 30
8.2.2 Messages datatypes and notations ..... 30
8.3 Station Association procedure ..... 30
8.3.1 General ..... 30
8.3.2 Public key certificates ..... 31
8.3.3 Configuration of authorized remote stations ..... 33
8.3.4 Pre-requisites to initiate the Station Association procedure ..... 33
8.3.5 Messages definition ..... 33
8.3.6 Controlling station state machine ..... 42
8.3.7 Controlled station state machine ..... 52
8.3.8 Verification of remote station’s certificate ..... 61
8.3.9 Verification of certificates during normal operations ..... 61
8.3.10 Update Keys derivation ..... 62
8.3.11 Controlling station directives for Station Association and Update Keys management ..... 63
8.3.12 Controlled station directives for Station Association and Update Keys management ..... 63
8.3.13 Initializing and updating Stations Association and Update Keys ..... 65
8.4 Session Key Change procedure ..... 66
8.4.1 General ..... 66
8.4.2 Messages definition ..... 67
8.4.3 Controlling station state machine ..... 76
8.4.4 Controlled station state machine ..... 85
8.4.5 Controlling station directives for Session Keys management ..... 93
8.4.6 Controlled station directives for Session Keys management ..... 93
8.4.7 Initializing and changing Session Keys ..... 94
8.5 Secure Data Exchange ..... 95
8.5.1 General ..... 95
8.5.2 Messages definition ..... 96
8.5.3 Controlling station state machine ..... 100
8.5.4 Controlled station state machine ..... 105
8.5.5 Controlling station directives for Secure Data Exchange ..... 109
8.5.6 Controlled station directives for Secure Data Exchange ..... 109
8.5.7 Example of Secure Data exchange during Station Association ..... 110
8.5.8 Example of Secure Data Exchange during Session Key Change ..... 111
9 Interoperability requirements ..... 113
9.1 Overview of clause ..... 113

9.2 Minimum requirements ..... 113
9.2.1 Overview of subclause ..... 113
9.2.2 Authentication algorithms ..... 113
9.2.3 Key wrap / transport algorithms ..... 113
9.2.4 Cryptographic keys ..... 114
9.2.5 Cryptographic curves ..... 114
9.2.6 Configurable values ..... 114
9.2.7 Cryptographic information ..... 116
9.3 Options ..... 116
9.3.1 Overview of subclause ..... 116
9.3.2 MAC/AEAD algorithms ..... 117
9.3.3 Key wrap / transport algorithms ..... 117
9.3.4 Cryptographic curves ..... 117
9.4 Use with TCP/IP ..... 117
9.5 Use with redundant channels ..... 117
10 Requirements for referencing this standard ..... 118
10.1 Overview of clause ..... 118
10.2 Selected options ..... 118
10.3 Message format mapping ..... 118
10.4 Reference to procedures ..... 118
10.5 Protocol information ..... 118
10.6 Controlled station response to unauthorized operations requests ..... 119
10.7 Transmission of security statistics ..... 119
10.8 Configurable values ..... 119
10.9 Protocol implementation conformance statement ..... 119
Annex A (informative) Security Event mapping to IEC 62351-14 ..... 120
A.1 General ..... 120
A.2 Mapping of IEC 62351-5 events specified in this document ..... 120
Bibliography ..... 122

Figure 1 – Overview of interaction between Central Authority and stations ..... 21
Figure 2 – Sequence of procedures ..... 23
Figure 3 – Station Association procedure ..... 34
Figure 4 – Station Association – Controlling station state machine ..... 43
Figure 5 – Station Association – Controlled station state machine ..... 53
Figure 6 – Example of Association ID, Update Keys and Session Keys initialization ..... 66
Figure 7 – Session Key Change procedure ..... 67
Figure 8 – Session Key Change – Controlling station state machine ..... 77
Figure 9 – Session Key Change – Controlled station state machine ..... 86
Figure 10 – Example of Session Key initialization and periodic update ..... 95
Figure 11 – Secure Data Exchange ..... 96
Figure 12 – Secure Data Exchange – Controlling station state machine ..... 101
Figure 13 – Secure Data Exchange – Controlled station state machine ..... 106
Figure 14 – Example of Secure Data Exchange during Station Association ..... 111
Figure 15 – Example of Secure Data messages exchanged during Session Key Change ..... 112

Table 1 – Scope of application to standards ..... 8
Table 2 – Summary of symmetric keys used ..... 19
Table 3 – Summary of asymmetric keys used ..... 19
Table 4 – States used in the controlling station state machine ..... 24
Table 5 – States used in the controlled station state machine ..... 24
Table 6 – Summary of timers and counters used ..... 25
Table 7 – Security statistics and associated events ..... 26
Table 8 – Elliptic curves ..... 31
Table 9 – Association Request message ..... 35
Table 10 – Association Response message ..... 36
Table 11 – Update Key Change Request message ..... 38
Table 12 – Data Included in MAC calculation (in order) ..... 40
Table 13 – Update Key Change Response message ..... 40
Table 14 – Data Included in MAC calculation (in order) ..... 41
Table 15 – Controlling station state machine: Station Association ..... 44
Table 16 – Controlled station state machine: Station Association ..... 54
Table 17 – List of pre-defined role-to-permission assignment ..... 64
Table 18 – Session Request message ..... 68
Table 19 – Session Response message ..... 70
Table 20 – Data Included in MAC calculation (in order) ..... 71
Table 20 – Session Key Change Request message ..... 72
Table 21 – Data Included in WKD (in order) ..... 73
Table 22 – Example of Session Key order ..... 74
Table 23 – Data Included in the MAC calculation (in order) ..... 74
Table 25 – Session Key Change Response message ..... 75
Table 26 – Data Included in the MAC calculation (in order) ..... 75
Table 27 – Controlling station state machine: Session Key Change ..... 78
Table 28 – Controlled station state machine: Session Key Change ..... 87
Table 29 – Secure Data message ..... 97
Table 29 – Secure Data Payload using MAC algorithm ..... 98
Table 31 – Data included in the MAC calculation in Secure Data Payload (in order) ..... 99
Table 32 – AEAD algorithm parameters to generate the Secure Data Payload (in order) ..... 99
Table 33 – Controlling station state machine: Secure Data Exchange ..... 102
Table 34 – Controlled station state machine: Secure Data Exchange ..... 107
Table 35 – Configuration of cryptographic information ..... 116
Table 36 – Legend for configuration of cryptographic information ..... 116
Table A.1 – Security event logs defined in IEC 62351-5 Ed.1 mapped to IEC 62351-14 ..... 120

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

## Part 5: Security for IEC 60870-5 and derivatives

## 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 62351-5 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is an International Standard.

This International Standard cancels and replaces IEC TS 62351-5 published in 2013. It constitutes a technical revision. The primary changes in this International Standard are:

a) The secure communication mechanism is performed on per controlling station/controlled station association.
b) User management to add, change or delete a User, was removed.
c) Symmetric method to change the Update Key was removed.
d) Asymmetric method to the change Update Key was reviewed.
e) Challenge/Reply procedure and concepts were removed.
f) Aggressive Mode concept was replaced with the Secure Data message exchange mechanism.
g) Authenticated encryption of application data was added.

h) The list of permitted security algorithms has been updated.

i) The rules for calculating messages sequence numbers have been updated

j) Events monitoring and logging was added.

NOTE The following print types are used:

CAPITALIZATION has been used in the text of this document to formally identify the most important components of the described security mechanism. These components include: 1) data items e.g. Update Keys, Session Keys; 2) procedure names, e.g. Station Association, Session Key Change; message names, e.g. Association Request, Session Request; 3) state names, e.g. Session Established, Wait for Session Response; 5) statistics e.g. Authentication Errors, Unexpected Messages and 5) event names e.g. Reply Timeout, Rx Invalid Session Key Change.

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

| Draft | Report on voting |
|---|---|
| 57/2516/FDIS | 57/2555/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/standardsdev/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.**

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

## Part 5: Security for IEC 60870-5 and derivatives

## 1 Scope

This part of IEC 62351 defines the application profile (A-profile) secure communication mechanism specifying messages, procedures and algorithms for securing the operation of all protocols based on or derived from IEC 60870-5, *Telecontrol Equipment and Systems – Transmission Protocols*. This document applies to at least those protocols listed in Table 1.

**Table 1 – Scope of application to standards**

| Number | Name |
|---|---|
| IEC 60870-5-101 | Companion standard for basic telecontrol tasks |
| IEC 60870-5-102 | Companion standard for the transmission of integrated totals in electric power systems |
| IEC 60870-5-103 | Companion standard for the informative interface of protection equipment |
| IEC 60870-5-104 | Network access for IEC 60870-5-101 using standard transport profiles |
| DNP3 | Distributed Network Protocol (defined in IEEE Std 1815, based on IEC 60870-1 through IEC 60870-5 and maintained jointly by the DNP Users Group and the IEEE) |

The initial audience for this document is intended to be the members of the working groups developing the protocols listed in Table 1.

For the measures described in this document to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process. The working groups in charge of taking this document to the specific protocols listed in Table 1 may choose not to do so.

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.

This document is organized working from the general to the specific, as follows:

- Clauses 2 through 4 provide background terms, definitions, and references.
- Clause 5 describes the problems this specification is intended to address.
- Clause 6 describes the mechanism generically without reference to a specific protocol.
- Clauses 7 and 8 describe the mechanism more precisely and are the primary normative part of this specification.
- Clause 9 define the interoperability requirements for this secure communication mechanism, including the relationship of this standard to IEC 62351-3 for transport layer security..
- Clause 10 describes the requirements for other standards referencing this document.

The actions of an organization in response to events and error conditions described in this document are expected to be defined by the organization's security policy and they are beyond the scope of this document.

## 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 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

IEC TS 62351-1, *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, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

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

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management*

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging*[1]

IETF RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

IETF RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption*

IETF RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

IETF RFC 7693, *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*

IETF RFC 7748, *Elliptic Curve for Security*

SEC2-V2, *Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain Parameters – Version 2.0*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN

[1] Under preparation. Stage at the time of publication: IEC ACDV 62351-14:2021.