IEC 62351-5

Edition 1.0 2023-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

https://standards.iteh.ai/catalog/standards/sist/109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023-01

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62351-100-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-100-5-2023

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

https://standards.iteh.ai/catalog/standards/sist/109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/[illegible]7a/iec-62351-5-2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
62351-5:2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62351-5:2023

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.

iTeh Standards
(standards.iteh.ai)
IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/iec/...-62351-5-2023

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

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*

iTeh STANDARD PREVIEW

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*

https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

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*

---

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
association ID
pair of values that uniquely identify the communication link between a controlling station and a controlled station and the related set of cryptographic keys

3.2
central authority
entity whose scope is the entire organization for which the purpose is to provide authentication information to devices and systems of the organization to authorize them to communicate. The Central Authority may or may not also be a Certificate Authority

3.3
communication link
the communication channel that connects two communicating entities. This link may be an actual physical link or it may be a logical link that uses one or more actual physical links.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.4
control direction
direction of transmission from the controlling station to a controlled station

IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

[SOURCE: IEC 60870-5-101:2003, 3.3]

3.5
controlled station
station which is monitored, or commanded and monitored by a master (controlling) station

Note 1 to entry: It is commonly called an "outstation" or "slave" in some specifications.

[SOURCE: IEC TR 60870-1-3:1997, 3, modified (addition of "(controlling" and Note 1 to entry)]

3.6
controlling station
station which performs the telecontrol of controlled stations

Note 1 to entry: It is commonly called a "master" or "master station" in some specifications.

[SOURCE: IEC TR 60870-1-3:1997, 3, modified (replacement of "outstations" with "controlled stations)]

3.7
local station
station nearest to the observer when the process is the same on both the controlling and controlled station

3.8
monitoring direction
direction of transmission from a controlled station to a controlling station

[SOURCE: IEC 60870-5-101:2003, 3.4]

3.9
remote station
station farther from the observer when the process is the same on both the controlling and controlled station

3.10
telecontrol
control of operational equipment at a distance using the transmission of information by telecommunication techniques

Note 1 to entry: Telecontrol may comprise any combination of command, alarm, indication, metering, protection and tripping facilities, without any use of speech messages.

[SOURCE: IEC TR 60870-1-3:1997, 3]

4 Abbreviated terms

Refer to IEC TS 62351-2 for a list of applicable abbreviated terms. The following terms are included here because they are specifically used in the affected protocols and also used in the discussion of this secure communication mechanism.

A-Profile	Application Profile. Security for the application layer.
AEAD	Authenticated Encryption with Associated Data. Function to encrypt and authenticate data (providing confidentiality and authentication). Note that AEAD also supports integrity protection of additional data, which is not encrypted.
AID	Association ID. Value identifying a single connection between controlling and Controlled stations.
ASDU	Application Service Data Unit. The application layer message submitted to lower layers for transmission.
C.ing	Controlling (referred to the controlling Station).
C.led	Controlled (referred to the controlled Station).
HKDF	HMAC-based Extract-and-Expand Key Derivation Function. Function to derive a symmetric cryptographic key.
HMAC	Keyed-Hash Message Authentication Code. Function to authenticate data using a secret cryptographic key.
IKM	Input Keying Material. Data provided to the HKDF-Extract function to generate a pseudo-random key (PRK).
KEK	Key Encryption Key. A secret key used to encrypt another secret key.
MAC	Message Authentication Code. The calculated value used by a station to authenticate and check the integrity of an Application Protocol Data Unit.
PRK	Pseudo-Random Key. Data provided to the HKDF-Expand function to generate a secret key.
T-Profile	Transport Profile. Security for transport layer (TCP/IP)
TCP/IP	Transmission Control Protocol/Internet Protocol.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

5 Problem description

5.1 Overview of clause

Clause 5 describes:

- the security threats that this document is intended to address;
- the unique design problems in implementing secure communication for IEC 60870-5 and derived protocols;
- the resulting design principles behind the mechanism.

5.2 Specific threats addressed

This document shall address only the following security threats, as defined in IEC TS 62351-2:

- spoofing;
- tampering;
- replay;
- eavesdropping

5.3 Design issues

5.3.1 Overview of subclause

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Subclause 5.3 describes the challenges faced in developing a secure communication proposal that can be applied to all the IEC 60870-5 and derived protocols. Subclause 5.3 is supplied for the benefit of security experts reviewing this document who may not be familiar with the electrical utility protocol environment.

IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-109f-4783-842e-2bb86f9ae67a/iec-62351-5-2023

5.3.2 Asymmetric communications

All the protocols affected by this specification share the concept of inequality between the communication stations. In each of these protocols there is a designated controlling station and a designated controlled station, each having different roles, responsibilities, procedures and message formats. In particular, the controlling station is in many cases responsible for flow control and media access control.

The existence of a definite controlled/controlling station designation has two impacts on the design of this secure communication mechanism:

- the format of messages in each direction will almost certainly differ, even if the functions are the same;
- Session key distribution is simplified because they will always be issued by the controlling station.

5.3.3 Message-oriented

All of the affected protocols are message-oriented. Connection authentication is done once to establish session keys, which in turn are used afterwards to support message authentication.

Message authentication must be performed on a message-by-message basis, rather than authenticating only at the beginning of a data stream and occasionally thereafter, as some connection-oriented protocols do.

5.3.4 Poor sequence numbers or no sequence numbers

A common security technique to address the threat of replay is to include in the message a sequence number. Combined with tests for message integrity, the sequence number makes it harder for an attacker to simulate a legitimate user by just copying an existing message, because the messages must be transmitted in a particular order.

Unfortunately, none of the affected protocols includes a sequence number that would provide adequate protection. Those sequence numbers that do exist have very low maximum values, permitting an attacker to attempt a replay after gathering only a small number of messages.

Therefore, the design of this specification must include its own sequence numbers and other time-varying data to protect against replay.

5.3.5 Limited processing power

The lack of processing power available on many power utility devices has been a major design concern for the affected protocols since their creation. This design requirement necessarily affects the secure communication mechanism also. The concern is heightened by the fact that many of these devices are single-processor machines; a denial-of-service attack would affect not only the communications capability of such devices but their function as an electrical control, protection, or monitoring device also.

Therefore, the use of security measures requiring extremely high processing power, such as public-key encryption and very large key sizes, has been avoided as much as possible.

iTeh Standards
(standards.iteh.ai)

5.3.6 Limited bandwidth

The limited amount of bandwidth available in utility networks has been the prime design concern (after message integrity) of the affected protocols. Links of 1 200 bits per second and lower are still a reality for many applications of these protocols. Some communication links also charge costs per octet transmitted.

IEC 62351-5:2023
https://standards.iteh.ai/catalog/standards/sist/d8247ab2-1691-4783-842e-2b686f9ac67a/iec-62351-5-2023

Therefore, the secure communication mechanism must not add very much overhead (i.e. few octets) to the affected protocols. The size of the additional authentication data has therefore been limited and truncated as much as possible while retaining an adequate level of security. Other measures may be taken in the implementations in each protocol.

5.3.7 No access to authentication server

The nature of the utility networks in which the affected protocols are deployed is that the controlling station is often the only device with which the controlled station can communicate. If there is any access to other networks, it is often achieved through the device implementing the controlling station.

The impact of this fact on the secure communication mechanism is that any system requiring on-line verification of the controlling station’s security credentials by a third party is not practical.

5.3.8 Limited frame length

Because of the restrictions on bandwidth and message integrity, the affected protocols are designed to send data in small frames of 255 octets or less. Some derivative protocols permit "chaining" frames together to create larger application layer messages.

However, in general, the secure communication mechanism cannot assume the transmission of large data units between the stations.