

# TECHNICAL SPECIFICATION

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

Withdrawn



**THIS PUBLICATION IS COPYRIGHT PROTECTED**  
**Copyright © 2013 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.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://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 corrigenda or an amendment might have been published.

#### Useful links:

IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - [webstore.iec.ch/csc](http://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: [csc@iec.ch](mailto:csc@iec.ch).



# TECHNICAL SPECIFICATION

IEC/TS 62351-5 Ed. 2.0 - Preview only Copy via ILNAS e-Shop

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

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

ICS 33.200

ISBN 978-2-83220-732-1

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## CONTENTS

|   |    |
|---|----|
| FOREWORD.....   | 6  |
| 1 Scope and object.....                                       | 8  |
| 2 Normative references .....                                  | 9  |
| 3 Terms and definitions .....                                 | 10 |
| 4 Abbreviated terms .....                                     | 11 |
| 5 Problem description (informative) .....                     | 11 |
| 5.1 Overview of clause .....                                  | 11 |
| 5.2 Specific threats addressed .....                          | 11 |
| 5.3 Design issues.....  | 11 |
| 5.3.1 Overview of subclause.....                              | 11 |
| 5.3.2 Asymmetric communications.....                          | 11 |
| 5.3.3 Message-oriented.....                                   | 12 |
| 5.3.4 Poor sequence numbers or no sequence numbers.....       | 12 |
| 5.3.5 Limited processing power.....                           | 12 |
| 5.3.6 Limited bandwidth.....                                  | 12 |
| 5.3.7 No access to authentication server.....                 | 12 |
| 5.3.8 Limited frame length.....                               | 13 |
| 5.3.9 Limited checksum.....                                   | 13 |
| 5.3.10 Radio systems.....                                     | 13 |
| 5.3.11 Dial-up systems.....                                   | 13 |
| 5.3.12 Variety of protocols affected.....                     | 13 |
| 5.3.13 Differing data link layers.....                        | 14 |
| 5.3.14 Long upgrade intervals.....                            | 14 |
| 5.3.15 Remote sites.....                                      | 14 |
| 5.3.16 Multiple users.....                                    | 14 |
| 5.3.17 Unreliable media.....                                  | 14 |
| 5.4 General principles.....                                   | 14 |
| 5.4.1 Overview of subclause.....                              | 14 |
| 5.4.2 Authentication only.....                                | 14 |
| 5.4.3 Application layer only.....                             | 15 |
| 5.4.4 Generic definition mapped onto different protocols..... | 15 |
| 5.4.5 Bi-directional.....                                     | 15 |
| 5.4.6 Challenge-response.....                                 | 15 |
| 5.4.7 Pre-shared keys as default option.....                  | 15 |
| 5.4.8 Backwards tolerance.....                                | 15 |
| 5.4.9 Upgradeable.....  | 16 |
| 5.4.10 Perfect forward secrecy.....                           | 16 |
| 5.4.11 Multiple users and auditing.....                       | 16 |
| 6 Theory of operation (informative).....                      | 16 |
| 6.1 Overview of clause.....                                   | 16 |
| 6.2 Narrative description .....                               | 16 |
| 6.2.1 Basic concepts .....                                    | 16 |
| 6.2.2 Initiating the challenge.....                           | 17 |
| 6.2.3 Replying to the challenge .....                         | 17 |
| 6.2.4 Authenticating .....                                    | 18 |
| 6.2.5 Authentication failure.....                             | 18 |

|        |   |    |
|--------|---|----|
| 6.2.6  | Aggressive mode .....   | 18 |
| 6.2.7  | Changing keys .....   | 18 |
| 6.2.8  | Security statistics .....   | 22 |
| 6.3    | Example message sequences .....   | 22 |
| 6.3.1  | Overview of subclause .....   | 22 |
| 6.3.2  | Challenge of a Critical ASDU .....                                      | 23 |
| 6.3.3  | Aggressive Mode .....   | 24 |
| 6.3.4  | Initializing and changing Session Keys .....                            | 24 |
| 6.4    | State machine overview .....  | 28 |
| 7      | Formal specification .....  | 32 |
| 7.1    | Overview of clause .....  | 32 |
| 7.2    | Message definitions .....   | 32 |
| 7.2.1  | Distinction between messages and ASDUs .....                            | 32 |
| 7.2.2  | Challenge message .....   | 33 |
| 7.2.3  | Reply message .....   | 35 |
| 7.2.4  | Aggressive Mode Request message .....                                   | 36 |
| 7.2.5  | MAC := OS8i[1..8i]; i:=specified by MALKey Status Request message ..... | 38 |
| 7.2.6  | Key Status message .....  | 38 |
| 7.2.7  | Session Key Change message .....  | 41 |
| 7.2.8  | Error message .....   | 43 |
| 7.2.9  | User Status Change message .....  | 45 |
| 7.2.10 | Update Key Change Request message .....                                 | 49 |
| 7.2.11 | Update Key Change Reply message .....                                   | 51 |
| 7.2.12 | Update Key Change message .....   | 52 |
| 7.2.13 | Update Key Change Signature message .....                               | 53 |
| 7.2.14 | Update Key Change Confirmation message .....                            | 54 |
| 7.3    | Formal procedures .....   | 55 |
| 7.3.1  | Overview of subclause .....   | 55 |
| 7.3.2  | Security statistics .....   | 56 |
| 7.3.3  | Challenger procedures .....   | 58 |
| 7.3.4  | Responder procedures .....  | 74 |
| 7.3.5  | Controlling station procedures .....                                    | 75 |
| 7.3.6  | Controlled station procedures .....                                     | 88 |
| 8      | Interoperability requirements .....                                     | 90 |
| 8.1    | Overview of clause .....  | 90 |
| 8.2    | Minimum requirements .....  | 90 |
| 8.2.1  | Overview of subclause .....   | 90 |
| 8.2.2  | MAC algorithms .....  | 90 |
| 8.2.3  | Key wrap / transport algorithms .....                                   | 91 |
| 8.2.4  | Fixed values .....  | 91 |
| 8.2.5  | Configurable values .....   | 91 |
| 8.3    | Options .....   | 96 |
| 8.3.1  | Overview of subclause .....   | 96 |
| 8.3.2  | MAC algorithms .....  | 96 |
| 8.3.3  | Encryption algorithms .....   | 98 |
| 8.3.4  | Key wrap / transport algorithms .....                                   | 98 |
| 8.3.5  | Configurable values .....   | 98 |
| 9      | Special Applications .....  | 99 |

|              |   |     |
|--------------|---|-----|
| 9.1          | Overview of clause .....  | 99  |
| 9.2          | Use with TCP/IP .....   | 99  |
| 9.3          | Use with redundant channels.....  | 99  |
| 9.4          | Use with external link encryptors .....                                   | 99  |
| 10           | Requirements for referencing this specification.....                      | 99  |
| 10.1         | Overview of clause .....  | 99  |
| 10.2         | Selected options.....   | 99  |
| 10.3         | Operations considered critical .....                                      | 100 |
| 10.4         | Addressing information.....   | 100 |
| 10.5         | Message format mapping .....  | 100 |
| 10.6         | Reference to procedures .....   | 100 |
| 11           | Protocol implementation conformance statement.....                        | 101 |
| 11.1         | Overview of clause .....  | 101 |
| 11.2         | Required algorithms .....   | 101 |
| 11.3         | MAC algorithms.....   | 101 |
| 11.4         | Key wrap algorithms.....  | 101 |
| 11.5         | Maximum Error messages sent.....  | 101 |
| 11.6         | Use of Error messages .....   | 101 |
| 11.7         | Update Key Change Methods .....   | 102 |
| 11.8         | User Status Change .....  | 102 |
| Annex A      | (informative) Compliance with ISO/IEC 11770.....                          | 103 |
| Bibliography | .....   | 109 |
| Figure 1     | – Overview of interaction between Authority and stations .....            | 22  |
| Figure 2     | – Example of successful Challenge of Critical ASDU .....                  | 23  |
| Figure 3     | – Example of failed Challenge of Critical ASDU .....                      | 23  |
| Figure 4     | – Example of a successful Aggressive Mode Request .....                   | 24  |
| Figure 5     | – Example of a failed Aggressive Mode Request.....                        | 24  |
| Figure 6     | – Example of Session Key initialization and periodic update.....          | 25  |
| Figure 7     | – Example of communications failure followed by Session Key change .....  | 26  |
| Figure 8     | – Example of successful User Status and Update Key Change .....           | 27  |
| Figure 9     | – User changes controlling stations.....                                  | 28  |
| Figure 10    | – Major state transitions for controlling station authentication.....     | 29  |
| Figure 11    | – Major state transitions for controlled station authentication .....     | 30  |
| Figure 12    | – Major state transitions for controlling station Update Key change ..... | 31  |
| Figure 13    | – Major state transitions for controlled station Update Key change .....  | 32  |
| Figure 14    | – Example Use of Challenge Sequence Numbers.....                          | 60  |
| Table 1      | – Scope of application to standards.....                                  | 8   |
| Table 2      | – Summary of symmetric keys used .....                                    | 18  |
| Table 3      | – Summary of asymmetric keys used (optional).....                         | 19  |
| Table 4      | – Challenge message.....  | 33  |
| Table 5      | – Reply message .....   | 35  |
| Table 6      | – Data Included in the MAC Value calculation .....                        | 36  |
| Table 7      | – Aggressive Mode Request message.....                                    | 36  |

|  |     |
|--|-----|
| Table 8 – Data Included in the MAC Value calculation in Aggressive Mode.....   | 37  |
| Table 9 – Key Status Request Message.....                                      | 38  |
| Table 10 – Use of Default Session Keys .....                                   | 38  |
| Table 11 – Key Status Message.....   | 39  |
| Table 12 – Data Included in the MAC Value Calculation for Key Status.....      | 41  |
| Table 13 – Key Change message.....   | 41  |
| Table 14 – Data Included in the key wrap (in order) .....                      | 42  |
| Table 15 – Example of key order.....   | 42  |
| Table 16 – Example of Wrapped Key Data.....                                    | 43  |
| Table 17 – Error message.....  | 43  |
| Table 18 – Creation of Certification Data .....                                | 46  |
| Table 19 – User Status Change message .....                                    | 46  |
| Table 20 – Update Key Change Request message.....                              | 50  |
| Table 21 – Update Key Change Reply message.....                                | 51  |
| Table 22 – Update Key Change message .....                                     | 52  |
| Table 23 – Encrypted Update Key Data .....                                     | 53  |
| Table 24 – Update Key Change Signature message .....                           | 53  |
| Table 25 – Data included in the Digital Signature.....                         | 54  |
| Table 26 – Update Key Change Confirmation message.....                         | 54  |
| Table 27 – Data included in the MAC calculation .....                          | 55  |
| Table 28 – States used in the state machine descriptions.....                  | 55  |
| Table 29 – Security statistics .....   | 57  |
| Table 30 – Challenger state machine.....                                       | 63  |
| Table 31 – User roles .....  | 77  |
| Table 32 – Controlling Station State Machine – Changing Session Keys.....      | 80  |
| Table 33 – Controlling Station State Machine – Changing Update Keys.....       | 84  |
| Table 34 – Special Statistic Event Thresholds.....                             | 92  |
| Table 35 – Algorithms and Messages used for each Update Key Change Method..... | 94  |
| Table 36 – Size of Challenge Data.....   | 94  |
| Table 37 – Configuration of Cryptographic Information.....                     | 95  |
| Table 38 – Legend for configuration of cryptographic information.....          | 96  |
| Table 39 – Construction of AES-GMAC initialization vector.....                 | 96  |
| Table 40 – Source of initialization vector components in each message.....     | 97  |
| Table A.1 – Cryptographic Notation .....                                       | 105 |
| Table A.2 – Compliance with ISO/IEC 11770 .....                                | 107 |

## 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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC/TS 62351-5, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This second edition cancels and replaces the first edition published in 2009. It constitutes a technical revision. The primary changes in the second edition are:

- adds the capability to change Update Keys remotely;
- adds security statistics to aid in detecting attacks;
- adds measures to avoid being forced to change session keys too often;
- discards unexpected messages more often as possible attacks;
- adds to the list of permitted security algorithms;
- adds new rules for calculating challenge sequence numbers.

The text of this technical specification is based on the following documents:

|               |                  |
|---------------|------------------|
| Enquiry draft | Report on voting |
| 57/1204/DTS   | 57/1282/RVC      |

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Capitalization has been used in the text of this specification 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) message names, e.g. Challenge, Reply, Aggressive Mode Request; 3) event names e.g. Reply Timeout, Rx Invalid Reply; 4) state names, e.g. Security Idle, Wait for Reply; and 5) statistics e.g. Authentication Failures, Unexpected Messages.

A list of all the 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 publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.