IEC/TS 62351-5

Edition 2.0 2013-04

TECHNICAL SPECIFICATION

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

CONTENTS

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.

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

Part 5: Security for IEC 60870-5 and derivatives

1 Scope and object

This part of IEC 62351 specifies 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 Technical Specification 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 (based on IEC 60870-1 through IEC 60870-5 and controlled by the DNP Users Group)

The initial audience for this Technical Specification is intended to be the members of the working groups developing the protocols listed in Table 1. For the measures described in this specification 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 subsequent audience for this specification is intended to be the developers of products that implement these protocols.

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

This part of IEC/TS 62351 focuses only on application layer authentication and security issues arising from such authentication. Other security concerns – in particular, protection from eavesdropping or man-in-the-middle attacks through the use of encryption – are considered to be outside the scope. Encryption may be added through the use of this specification with other specifications.

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 describes a few particular implementation issues that are special cases.
- Clause 10 describes the requirements for other standards referencing this specification.

- Clause 11 describes the Protocol Implementation Conformance Statement (PICS) for this mechanism.

Unless specifically labelled as informative or optional, all clauses of this specification are normative.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 – 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/TS 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/TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

ISO/IEC 9798-4, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*

ISO/IEC 11770-2:2008, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

FIPS 180-2, *Secure Hash Standard* (includes SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512). USA NIST

FIPS 186-2, *Digital Signature Standard (DSS),* USA NIST, February 2000 including Change Notice #1, October 2001. Used for the random number generation algorithms in the Appendix

FIPS 186-3, *Digital Signature Standard (DSS),* USA NIST, June 2009. Used for digital signature algorithms when asymmetric Update Key change is implemented

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

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

RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

RFC 3629, *UTF-8, a transformation format of ISO 10646*

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

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*