

TECHNICAL SPECIFICATION

IEC TS 62351-3

First edition
2007-06

**Power systems management and
associated information exchange –
Data and communications security –**

**Part 3:
Communication network and system security –
Profiles including TCP/IP**



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE

K

For price, see current catalogue

CONTENTS

FOREWORD.....	3
1 Scope and object.....	5
1.1 Scope.....	5
1.2 Object	5
2 Normative references	6
3 Terms and definitions	6
4 Security issues addressed by this technical specification.....	6
4.1 Operational requirements affecting the use of TLS in the telecontrol environment	6
4.2 Security threats countered.....	7
4.3 Attack methods countered	7
5 Mandatory requirements	7
5.1 Deprecation of non-encrypting cipher suites	7
5.2 Negotiation of versions	7
5.3 Cipher renegotiation	7
5.4 Message authentication code	8
5.5 Certificate support.....	8
5.5.1 Multiple Certificate Authorities (CAs)	8
5.5.2 Certificate size	8
5.5.3 Certificate exchange.....	8
5.5.4 Certificate comparison	8
5.6 Co-existence with non-secure protocol traffic	9
6 TC 57 referencing standard requirements	9
7 Conformance.....	10

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 3: Communication network and system security – Profiles including TCP/IP

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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 62351-3, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/803/DTS	57/857/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.

A list of all parts of 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 maintenance result 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 3: Communication network and system security – Profiles including TCP/IP

1 Scope and object

1.1 Scope

This part of IEC 62351, which is a technical specification, specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer.

Although there are many possible solutions to secure TCP/IP, the particular scope of this part is to provide security between communicating entities at either end of a TCP/IP connection within the end communicating entities. The use and specification of intervening external security devices (e.g. “bump-in-the-wire”) are considered outside the scope of this technical specification.

1.2 Object

This part of IEC 62351 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 2246) so that they are applicable to the telecontrol environment of IEC TC 57. It is intended that this specification be referenced as a normative part of other IEC TC 57 standards that have the need for providing security for their TCP/IP-based protocol. However, it is up to the individual protocol security initiatives to decide if this technical specification is to be referenced.

This part reflects the security requirements of the IEC TC 57 protocols. Should other standards bring forward new requirements, this specification may need to be revised.

The initial audience for this specification is intended to be the members of the working groups developing or making use of the protocols within IEC TC 57. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves, where the protocols make use of TCP/IP. This specification 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.

2 Normative references

The following referenced documents are indispensable for the application 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 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 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

RFC 2246:1999, *The TLS Protocol Version 1.0*¹⁾

RFC 2712:1999, *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*²⁾

RFC 3268, 2002, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*

RFC 3280, 2002, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

¹⁾ T. Dierks, C. Allen. This standard is typically referred to as SSL/TLS.

²⁾ A. Medvinsky, M. Hur.