TECHNICAL SPECIFICATION

IEC TS 62351-4

First edition
2007-06

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

Part 4: Profiles including MMS

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE P

For price, see current catalogue

CONTENTS

FOREWORD 3

1 Scope and object 5
1.1 Scope 5
1.2 Object 5
2 Normative References 5
3 Terms and definitions 6
4 Security issues addressed by this technical specification 6
4.1 Security for application and transport profiles 6
4.2 Security threats countered 7
4.3 Attack methods countered 7
5 A-Profile security 7
5.1 MMS 8
5.2 Logging 8
5.3 ACSE 8
5.3.1 Peer entity authentication 8
5.3.2 AARQ 11
5.3.3 AARE 11
6 T-Profile security 11
6.1 TCP T-Profiles 11
6.1.1 Conformance to this technical specification 11
6.1.2 Use of TLS in TCP T-Profiles 11
6.1.3 TP0 12
6.1.4 RFC 1006 13
6.1.5 TLS requirements 13
6.1.6 Use of TLS 13
6.2 OSI T-Profiles 14
6.3 Certificate authority support 15
7 Conformance 15
7.1 General conformance 15
7.2 Conformance of IEC 60870-6 TASE.2 security 15

Bibliography 16

Figure 1 – Application and transport profiles 7
Figure 2 – Non-secure and secure TCP T-Profiles IEC 62351 12

Table 1 – TP0 maximum sizes 12
Table 2 – Recommended cipher suite combinations 14
Table 3 – Supported cipher suites 15

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 4: Profiles including MMS

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 62351-4, 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
57/804/DTS	57/858/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 4: Profiles including MMS

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies procedures, protocol extensions, and algorithms to facilitate securing ISO 9506 – Manufacturing Message Specification (MMS) based applications. It is intended that this technical specification be referenced as a normative part of other IEC TC 57 standards that have the need for using MMS in a secure manner.

This technical specification represents a set of mandatory and optional security specifications to be implemented for applications when using ISO/IEC 9506 (Manufacturing Automation Specification).

NOTE Within the scope of IEC TC 57, there are two identified standards that may be impacted: IEC 61850-8-1 and IEC 60870-6.

This specification contains a set of specifications that are to be used by referencing standards in order to secure information transferred when using MMS. The recommendations are based upon specific communication profile protocols used in order to convey MMS information.

IEC 61850-8-1 and IEC 60870-6 make use of MMS in a 7-layer connection-oriented mechanism. Each of these standards is used over either the OSI or TCP profiles.

1.2 Object

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 ISO 9506. 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.

2 Normative References

IEC 60870-6 (all parts), *Telecontrol equipment and systems*

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

ISO/IEC 9594-8:2005 /ITU-T Recommendation X.509:2005*, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*

RFC 1006, *ISO Transport Service on top of the TCP Version: 3*

RFC 2313, *PKCS #1: RSA Encryption Version 1.5*

RFC 2246, *The TLS Protocol, Version 1.0*

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