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

Reference number
IEC/TS 62351-4:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

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

CONTENTS

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions contained in IEC 62351-2 as well as the following terms and definitions apply.

3.3
bilateral agreement
agreement between two control centres which includes the data elements to be accessed and the means to access them.

[IEC 60870-6-503:2002, definition 3.3]

3.4
bilateral table
computer representation of the bilateral agreement. The representation used is a local matter

[IEC 60870-6-503:2002, definition 3.4]

4 Security issues addressed by this technical specification

4.1 Security for application and transport profiles

The communication security, specified in this specification, shall be discussed in terms of:

- application profiles: an A-Profile defines the set of protocols and requirements for layers 5-7 of the OSI Reference Model;
- transport profiles: a T-Profile defines the set of protocols and requirements for layers 1-4 of the OSI Reference Model.

There have been one (1) A-Profile and two (2) T-Profiles identified within the TC 57 context. This specification shall specify security extensions for all of the identified profiles. (See Figure 1.)

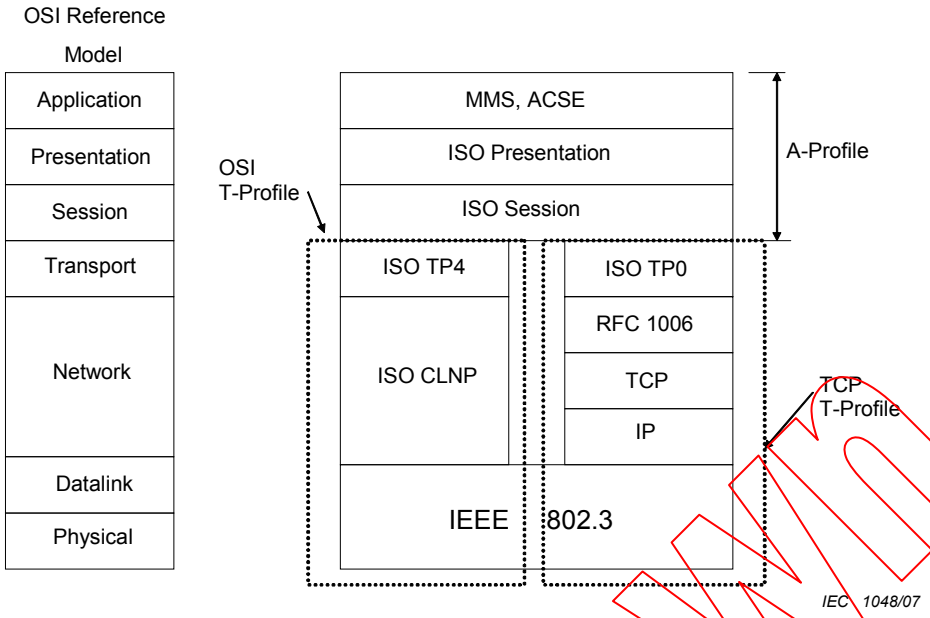

Figure 1 – Application and transport profiles

4.2 Security threats countered

See IEC 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this part include:

- unauthorized access to information.

If IEC 62351-3 is employed, then the specific threats countered in this part include:

- unauthorized access to information through message level authentication and encryption of the messages;
- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specification/recommendations found within this document. The following list is exclusive of the attack methods countered through IEC 62351-3. In the case that IEC 62351-3 is not employed, the threats countered are restricted to protection during association establishment:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;
- tamper detection/message integrity: these threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;
- replay: this threat will be countered through the use of specialized processing state machines specified within this specification.

5 A-Profile security

The following clauses specify the application profiles (A-Profiles) that shall be supported for implementations claiming conformance to this specification.

5.1 MMS

The implementation of MMS must provide some mechanism for configuring and making use of the capabilities of the secure profile. In general, the following needs to be provided.

- A mechanism for configuration of certificate information and the binding of that information to access authentication (e.g., the bilateral tables).
- A mechanism for configuration of the acceptable incoming association profile for the implementation's access control mechanism. It is suggested that the following choices be provided:
  - DON'T_CARE: would indicate either a secure or non-secure profile would be allowed to establish a MMS association.
  - NON_SECURE: would indicate that the non-secure profile must be used in order to allow establishment of a MMS association.
  - SECURE: would indicate that the secure profile must be used in order to allow establishment of a MMS association.
- A mechanism for configuration of the profile to use in order to initiate a MMS association. It is suggested that the following choices be provided:
  - NON_SECURE: would indicate that the non-secure profile must be used in order to allow establishment of a MMS association.
  - SECURE: would indicate that the non-secure profile must be used in order to allow establishment of a MMS association.
- A mechanism to convey/verify the association parameters. These parameters should include: presentation address; profile used indication (e.g., secure or non-secure); and ACSE authentication parameters. The indication of the use of a "secure profile" shall be reserved if the secure transport layer, as set forth within this document, has been negotiated as part of the MMS association[1].

  This information shall be used, in conjunction with the configured MMS expected association values, to determine if a MMS association should be established. The entity that determines the actual acceptance is a local issue.

It is a mandatory requirement that changes in the configuration parameters, discussed above, not require all MMS associations to be terminated in order for the configuration changes to take affect.

It is strongly suggested that a MMS implementation log events and information associated with rejected associations that were rejected due to security violations.

5.2 Logging

It is important that care be taken to log security related violations in a separate log whose contents is inherently secure from manipulation (e.g., modification of information or deletion of information). Implementers should strive to archive enough information so that security audit and prosecution is facilitated. The actual implementation of this recommendation is a local issue.

5.3 ACSE

5.3.1 Peer entity authentication

Peer entity authentication shall occur at association set-up time. Authentication information shall be carried in the calling-authentication-value and responding-authentication-value fields of the authentication functional unit (FU) of the ACSE AARQ and AARE PDUs respectively.

---

[1] This allows for the ACSE authentication to be used over either the secure or non-secure profiles to achieve stronger authentication.