

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

Part 4: Profiles including MMS

ICS 33.200

National foreword

This Draft for Development is the UK implementation of IEC/TS 62351-4:2007.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 July 2007

© BSI 2007

ISBN 978 0 580 56446 8

Amendments issued since publication

Amd. No.	Date	Comments

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)

CONTENTS

1	Scope and object.....	3
1.1	Scope.....	3
1.2	Object	3
2	Normative References	3
3	Terms and definitions	4
4	Security issues addressed by this technical specification.....	4
4.1	Security for application and transport profiles	4
4.2	Security threats countered.....	5
4.3	Attack methods countered	5
5	A-Profile security	5
5.1	MMS	6
5.2	Logging	6
5.3	ACSE	6
5.3.1	Peer entity authentication	6
5.3.2	AARQ	9
5.3.3	AARE	9
6	T-Profile security	9
6.1	TCP T-Profiles.....	9
6.1.1	Conformance to this technical specification	9
6.1.2	Use of TLS in TCP T-Profiles.....	9
6.1.3	TP0	10
6.1.4	RFC 1006	11
6.1.5	TLS requirements	11
6.1.6	Use of TLS	11
6.2	OSI T-Profiles	12
6.3	Certificate authority support	13
7	Conformance.....	13
7.1	General conformance	13
7.2	Conformance of IEC 60870-6 TASE.2 security	13
	Bibliography.....	14
	Figure 1 – Application and transport profiles	5
	Figure 2 – Non-secure and secure TCP T-Profiles IEC 62351	10
	Table 1 – TP0 maximum sizes	10
	Table 2 – Recommended cipher suite combinations.....	12
	Table 3 – Supported cipher suites.....	13

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.)