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 It also gives information on projects, withdrawn and replaced publications.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.)

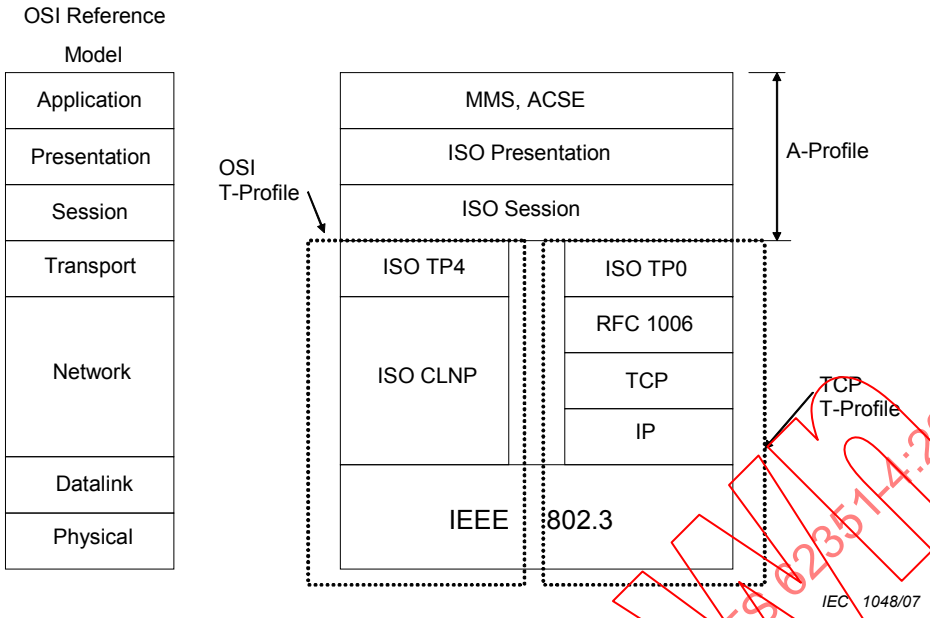

Figure 1 – Application and transport profiles

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.

The bit strings for the sender-ACSE-requirements and responder-ACSE-requirements fields of the authentication FU shall be DEFAULTED to include the authentication FU, when ACSE security is in use. Otherwise, the bits shall be DEFAULTED to exclude the authentication FU (this provides backward compatibility).

The calling-authentication-value and responding-authentication-value fields are of type authentication-value that is further defined in ISO 8650 as a CHOICE. The CHOICE for the Authentication-value shall be EXTERNAL. The presentation context shall include a reference to the abstract syntax that is used for the EXTERNAL.

The ACSE mechanism-name field shall be used to denote the format of the authentication-value field being conveyed. The definition of the mechanism-name field (both for AARQ and AARE) shall be:

The ICCP authentication value (following) shall be carried in the authentication-value field of the authentication FU of ACSE. This value shall be used when peer entity authentication is required. The value shall be carried as the “external” as defined by the ACSE authentication-value production (replicated below) as a SingleASN1Type.

NOTE The following production is a reproduction from ISO/IEC 8650 and is for informative purposes only.

```
Authentication-value::= CHOICE {

        charstring  [0] IMPLICIT GraphicString,
        bitstring   [1] IMPLICIT BIT STRING,
        external    [2] IMPLICIT EXTERNAL,
         other  [3] IMPLICIT SEQUENCE {other-mechanism-name
                        MECHANISM-NAME.&id({ObjectSet}),
                    other-mechanism-value
                        MECHANISM-NAME.&Type
                }
    }



    STASE-MMS-Authentication-value {iso member-body usa(840) ansi-t1-259-1997(0)
    stase(1) stase-authentication-value(0) abstractSyntax(1) version1(1)}

    DEFINITIONS IMPLICIT TAGS::= BEGIN

    -- EXPORTS everything

    IMPORTS

    SenderId, ReceiverId, Signature, SignatureCertificate

    FROM ST-CMIP-PCI {iso member-body usa(840) ansi-t1-259-1997(0) stase(1) stase-
    pci(1) abstractSyntax(4) version1(1)};

    MMS_Authentication-value::= CHOICE{
            certificate-based [0] IMPLICIT SEQUENCE {
            authentication-Certificate [0] IMPLICIT &SignatureCertificate,
            time [1] IMPLICIT GENERALZEDTIME,
            signature [2] IMPLICIT &SignedValue
            },

...}
END
```

&SignatureCertificate

SignatureCertificate::= OCTET STRING -- size shall have a minimum-maximum size of 8192 octets.

The contents of the SignatureCertificate OCTET STRING shall be a Basic Encoding Rules encoded X.509 certificate (specified in CMIP). The certificate exchange shall be bi-directional and shall provide an individual certificate from a configured and trusted certificate authority. If any of these conditions are not met, the connection shall be terminated appropriately.

Identification of individual certificates shall be based upon the certificate Subject, as a minimum.

In order to achieve interoperability of certificates, it is necessary to set a maximum allowed size for the certificates exchanged by ACSE. This size shall be limited to a maximum encoding size of 8192 octets.

It is a local issue if a larger certificate can be accepted.

If the certificate size exceeds the minimum-maximum (e.g. 8192) or the local maximum, then the connection shall be refused and a disconnect shall occur.

&SignedValue

The value of the SignedValue shall be the value of the time field signed as specified by the PKCS#1 Version 2. The value is the encoded GENERALZEDTIME string but does not include the ASN1 tag or length. This value shall be signed per the RSA signing algorithm in the specification. A key length of 1024 bits shall be supported as a minimum-maximum.

The definition of the SignedValue shall be governed by the DigitalSignature definition found in RFC 2313:

> "For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature."
>
> NOTE The reference to MD5, in the definition, is not normative. It is an example given in the RFC 2313 quoted text. The actual algorithm is specified in the following paragraph to be SHA1.

RFC 3447 (specification for PKCS#1 Version 2) specifies RSASSA-PKCS1-v1_5 as the signature algorithm. This is the algorithm that shall be used by implementations claiming conformance to this specification. The use of RFC 3447 shall be restricted to those abilities/capabilities that are compatible with PKCS Version 1.5 (RFC 2313). The Hash algorithm shall be SHA1.

time

This parameter shall be the GENERALIZEDTIME representation of the GMT value of the time at which the authentication-value was created.

The accuracy of this time is a local issue but shall be as accurate as possible. It is equally valid to determine the value of the time parameter during the invocation of the MMS Intiate. Request service, Initiate.Response service, or during the encoding of the ACSE PDUs for those services.

5.3.2 AARQ

The sender of an AARQ shall encode the appropriate ACSE AuthenticationMechanism and AuthenticationValue fields and send the AARQ through the use of the Presentation-Connect service.

The receiver of an AARQ-indication shall use the AuthenticationMechanism and AuthenticationValue fields to attempt to verify the signed value. If the decoded signed value is not equal to the value of the time field then the receiver shall cause a P-ABORT to be issued. If the time field value is more than 10 min[2)] difference from the local time, the receiver shall cause a P-ABORT to be issued.

If the receiver of the AARQ has received an AARQ containing the same signed value within the last 10 min, then the receiver shall cause a P-ABORT to be issued.

If the signed value has not caused a P-ABORT, then the signed value and other security parameters shall be passed to the ACSE user (e.g., MMS or TASE.2 or the local Application). The method by which these parameters are passed is a local issue.

5.3.3 AARE

The sender of an AARE shall encode the appropriate ACSE AuthenticationMechanism and AuthenticationValue fields and send the AARE through the use of the Presentation-Connect service.

The receiver of an AARE-indication shall use the AuthenticationMechanism and AuthenticationValue fields to attempt to verify the signed value. If the decoded signed value is not equal to the value of the time field then the receiver shall cause a P-ABORT to be issued. If the time field value is more than 10 min[3)] difference from the local time, the receiver shall cause a P-ABORT to be issued.

If the receiver of the AARE has received an AARE containing the same signed value within the last 10 min, then the receiver shall cause a P-ABORT to be issued.

If the signed value has not caused a P-ABORT, then the signed value and other security parameters shall be passed to the ACSE user (e.g., MMS or TASE.2 or the local Application). The method by which these parameters are passed is a local issue.

6 T-Profile security

6.1 TCP T-Profiles

6.1.1 Conformance to this technical specification

An implementation that claims conformance to this technical specification shall support security for the TCP T-Profile.

6.1.2 Use of TLS in TCP T-Profiles

The security recommendations for the TCP T-Profile do not attempt to specify security recommendations for TCP, IP, or Ethernet. Rather the specifications within this specification specify how to properly use Transport Layer Security and the securing of RFC 1006.

---

2) This means that there is a window of vulnerability of 10 min in which the same signed value could be used by an attacker.

3) This means that there is a window of vulnerability of 10 min in which the same signed value could be used by an attacker.

The security TCP T-Profile inserts makes use of TLS (as specified by RFC 2246) to provide encryption and nodal authentication prior to RFC 1006.

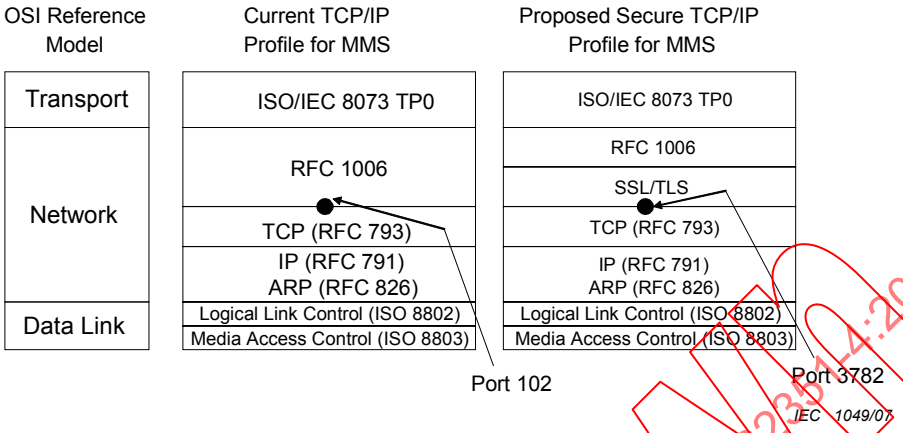

Figure 2 – Non-secure and secure TCP T-Profiles IEC 62351

Figure 2 shows the two relevant TCP T-Profiles. One is the standard non-secure RFC 1006 T-Profile as specified by IETF. The other is the secure RFC 1006 profile that is specified within this technical specification.

6.1.3 TP0

6.1.3.1 Enforcement of maximum lengths

TP0 specifies the maximum size of TPDU. It is recommended that implementations use Table 1 to make sure that the RFC 1006 length does not exceed the maximum size. It is a local issue in regards to the processing of a TPDU whose RFC 1006 size is incorrect.

Table 1 – TP0 maximum sizes

OSI TP0 primitive	RFC 1006 header	ISO TP0 LI field		ISO TP0 user data		RFC 1006 length range	
	Octets	Minimum	Maximum	Minimum	Maximum	Mimum	Maximum
CR	4	7	254	0	0	11	258
CC	4	7	254	0	0	11	258
DR	4	7	254	0	0	11	258
DC	4	7	254	0	0	11	258
DT	4	3	3	1	2048 [a]	8	2055
ER	4	5	254	0	0	9	259
ED	Not allowed due to TP0 restriction						
AK	Not allowed due to TP0 restriction						
EA	Not allowed due to TP0 restriction						
RJ	Not allowed due to TP0 restriction						
[a] Maximum based upon negotiation of CR/CC exchange. 128 octets is the minimum allowed.							

6.1.3.2 Response to TP0 unsupported TPDUs

It is recommended that the reception of an ED, AK, EA, or RJ TPDU be ignored.

6.1.3.3 Transport selectors

The International Standardized Profiles (ISP) for MMS specify that the transport selectors (TSELs) shall have a maximum size of 32 octets. However, the parameterization of the selector according to ISO/IEC 8073 may have a length of 255 octets.

An implementation that receives a TSEL whose length is greater than 32 octets shall cause the connection to be aborted.

6.1.4 RFC 1006

It is recommended that the following enhancements be made to an RFC 1006 implementation when it is used in either the secure or non-secure T-Profile.

6.1.4.1 Version number

The local implementation shall ignore the value of the RFC 1006 version field value. Local processing of the OSI TPDU(s) shall continue as if the field value were 3.

6.1.4.2 Length

The RFC 1006 length field shall be limited to a value of no greater than 2056 octets. This length corresponds to the maximum TP0 TPDU allowed (e.g. 2048 octets).

The processing of a length that is greater than 2056 octets is a local issue. However it is strongly suggested to disconnect the connection.

6.1.4.3 Keep-alive

Implementations that claim conformance to this specification shall make use of the TCP-KEEPALIVE function. The timeout function should be set to approximately 1 min, or less.

6.1.5 TLS requirements

6.1.5.1 TCP port usage

The non-secure T-Profile shall use TCP port 102 as specified by RFC 1006.

Implementations claiming conformance to this specification shall use TCP port 3782 to indicate the use of the secure TCP T-Profile.

6.1.5.2 Simultaneous support

The following requirement applies to implementations that claim support for more than one simultaneous MMS association. For such implementations, it shall be possible to communicate via the secure and non-secure T-Profiles simultaneously.

6.1.6 Use of TLS

Transport Layer security shall be used as specified by IEC 62351-3.

6.1.6.1 Disabling of TLS

Implementations shall permit TLS to be disabled.

6.1.6.2 Cipher renegotiation

An implementation that claims conformance to this specification shall support minimum-maximum renegotiation if either: five-thousand (5000) ISO TPUs have been sent or 10 min have elapsed from the previous renegotiation.

6.1.6.3 Certificate size

An implementation that claims conformance to this specification shall support a minimum-maximum certificate size of 8192 octets. It is a local issue if larger certificates are supported.

An implementation that receives a certificate larger than the size that it can support shall terminate the connection.

6.1.6.4 Certificate revocation

The default evaluation period for revoked certificates shall be 12 h. This evaluation period shall be configurable.

An implementation that claims conformance to this specification shall terminate a connection where one of the certificates used to establish the connection is revoked.

6.1.6.5 Mandatory and recommended cipher suites

All implementations that claim conformance to this specification shall support TLS_DH_DSS_WITH_AES_256_SHA at a minimum.

Other standards that reference this specification may add additional mandatory cipher suites.

It is recommended that the TLS cipher suites listed in Table 2 be considered for use.

Table 2 – Recommended cipher suite combinations

Key exchange		Encryption	Hash
Algorithm	Signature		
TLS_RSA_		WITH_RC4_128_	SHA
TLS_RSA_		WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA
TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA
TLS_DH_	DSS_	WITH_AES_128_	SHA
TLS_DH_	DSS_	WITH_AES_256_	SHA
TLS_DH_		WITH_AES_128_	SHA
TLS_DH_		WITH_AES_256_	SHA

NOTE The negotiation mechanism in TLS selects the actual cipher suite used for a particular connection based upon the configured allowed/present cipher suites.

6.2 OSI T-Profiles

The security of OSI T-Profiles is outside the scope of this specification.