

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Power systems management and associated information exchange – Data and communications security –
Part 4: Profiles including MMS and derivatives**

**Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 4: Profils comprenant le MMS et ses dérivés**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-8621-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

REDLINE VERSION

VERSION REDLINE

**Power systems management and associated information exchange – Data and communications security –
Part 4: Profiles including MMS and derivatives**

**Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 4: Profils comprenant le MMS et ses dérivés**

CONTENTS

FOREWORD	8
1 Scope	10
1.1 General	10
1.2 Code components	11
2 Normative references	11
3 Terms, definitions and abbreviated terms	12
3.1 General	12
3.2 Terms and definitions	13
3.3 Abbreviated terms	16
4 Security issues addressed by this part of IEC 62351	18
4.1 Communications reference models	18
4.2 Security for application and transport profiles	18
4.3 Compatibility and native modes	19
4.4 Security threats countered	19
4.4.1 General	19
4.4.2 Threats countered in compatibility mode	20
4.4.3 Threats countered in native mode	20
4.5 Attack methods countered	20
4.5.1 General	20
4.5.2 Attacks countered in compatibility mode	20
4.5.3 Attacks countered in native mode	20
4.6 Logging	21
5 Specific requirements	21
5.1 Specific requirements for ICCP/IEC 60870-6-x communication stack	21
5.2 Specific requirements for IEC 61850	22
6 Transport Security	22
6.1 General	22
6.2 Application of transport layer security (TLS)	22
6.2.1 General	22
6.2.2 The TLS cipher suite concept	23
6.2.3 TLS session resumption	23
6.2.4 TLS session renegotiation	23
6.2.5 Supported number of trust anchors	23
6.2.6 Public-key certificate size	23
6.2.7 Evaluation period for revocation state of public-key certificates	23
6.2.8 Public-key certificate validation	24
6.2.9 Security events handling	24
6.3 T-security in an OSI operational environment	24
6.3.1 General	24
6.3.2 TCP ports	24
6.3.3 Disabling of TLS	25
6.3.4 TLS cipher suites support	25
6.4 T-security in an XMPP operational environment	27
7 Application layer security overview (informative)	27
7.1 General	27
7.2 Description techniques	28

7.2.1	General	28
7.2.2	ASN.1 as an XML schema definition	28
7.2.3	W3C XML Schema Definition (W3C XSD)	28
7.2.4	XML namespace	29
8	Use of cryptographic algorithms	29
8.1	General.....	29
8.2	Basic cryptographic definitions.....	29
8.3	Public-key algorithms.....	30
8.4	Hash algorithms.....	31
8.5	Signature algorithms	31
8.6	Symmetric encryption key algorithms used for encryption only	31
8.7	Authenticated encryption algorithms	32
8.8	Integrity check value algorithms	32
9	Object identifier allocation (normative).....	33
10	General OSI upper layer requirements (normative)	33
10.1	Overview.....	33
10.2	General on OSI upper layer requirements	34
10.3	Session protocol requirements	34
10.4	Presentation protocol requirements.....	35
10.4.1	Context list	35
10.4.2	Abstract syntaxes	35
10.4.3	Presentation user data.....	36
10.4.4	ASN.1 encoding requirements	36
10.5	Association control service element (ACSE) protocol requirements	37
10.5.1	General	37
10.5.2	Protocol version.....	37
10.5.3	Titles	37
10.5.4	Use of ASN.1 EXTERNAL data type	38
11	A-security profile (normative).....	38
11.1	OSI requirements specific to A-security profile	38
11.1.1	General	38
11.1.2	Additional session protocol requirements.....	38
11.1.3	Additional presentation protocol requirement	38
11.1.4	Additional ACSE requirements.....	39
11.2	MMS Authentication value.....	41
11.2.1	General	41
11.2.2	MMS-Authentication value data type.....	41
11.2.3	Handling of the association request (AARQ-apdu)	42
11.2.4	Handling of the association result (AARE-apdu).....	42
12	End-to-end application security model	43
12.1	Introduction and general architecture	43
12.2	Abstract syntax specifications	45
12.2.1	General	45
13	End-to-end application security (normative).....	45
13.1	Association management	45
13.1.1	General concept	45
13.1.2	UTC time specification.....	45
13.1.3	Handshake request.....	46

13.1.4	Handshake accept	47
13.1.5	Association reject by the protected protocol	47
13.1.6	Association reject due to security issues	48
13.1.7	Handshake security abort	48
13.1.8	Data transfer security abort	48
13.1.9	Abort by protected protocol	49
13.1.10	Association release request	49
13.1.11	Association release response	50
13.2	Data transfer phase	50
13.2.1	General	50
13.2.2	Clear data transfer	50
13.2.3	Encrypted data transfer	50
13.3	ClearToken data types	51
13.3.1	The ClearToken1 data type	51
13.3.2	The ClearToken2 data type	58
13.3.3	The ClearToken3 data type	59
13.4	Authentication and integrity specifications	60
13.4.1	The Signature data type	60
13.4.2	The authenticator data type	60
14	E2E security error handling (normative)	61
14.1	General	61
14.2	Specification of diagnostics	61
14.2.1	Handshake diagnostics	61
14.2.2	The data transfer diagnostics	63
14.3	Checking of E2E-security handshake request and accept	64
14.3.1	General	64
14.3.2	Signature checking	64
14.3.3	Protected protocol identity checking	65
14.3.4	ClearToken1 checking	65
14.4	Checking of security protocol control information during data transfer	67
14.4.1	General	67
14.4.2	Authenticator checking	67
14.4.3	Checks of the ClearToken2 value	67
15	E2E security used in an OSI operational environment	68
15.1	General	68
15.2	Additional upper layer requirements	68
15.2.1	Additional presentation layer requirements	68
15.2.2	Additional ACSE requirements	68
15.3	Association management in an OSI operational environment	69
15.3.1	General	69
15.3.2	Mapping to ACSE association request	69
15.3.3	Mapping to ACSE association response	69
15.3.4	Mapping to ACSE abort	70
15.3.5	Mapping to ACSE release request	71
15.3.6	Mapping to ACSE release response	71
15.4	Data transfer in OSI operational environment	71
15.4.1	General	71
15.4.2	Mapping of the clear data transfer SecPDU	71
15.4.3	Mapping of the encrypted data transfer SecPDU	72

15.5	OSI upper layer routing	72
15.6	OSI operational environment checking	74
15.6.1	General checking	74
15.6.2	Environment mapping checking	75
15.6.3	OSI operational environment diagnostics	75
16	E2E security used in in an XMPP operational environment	75
16.1	General on wrapping to an XMPP operational environment	75
16.2	Mapping of SecPDUs to iq stanzas	76
16.3	Mapping of SecPDUs to message stanzas	77
16.4	XMPP stanza error handling	77
16.5	XML namespaces	78
16.6	Encoding of EnvPDUs within XMPP stanzas	78
16.7	Multiple associations	79
16.8	Release collision consideration	79
17	Conformance to this document	79
17.1	General	79
17.2	Notation	79
17.3	Conformance to operational environment	80
17.4	Conformance to modes of operation	80
17.5	Conformance to compatibility mode	80
17.6	Conformance to native mode	81
Annex A	(normative) Formal ASN.1 specification for the A-security-profile	83
Annex B	(normative) Formal ASN.1 specification for the End-to-End security	84
Annex C	(normative) Formal W3C XSD specification for the end-to-end security	95
Annex D	(normative) ASN.1 module for OSI operational environment	110
D.1	Scope of annex	110
D.2	ASN.1 module	110
Annex E	(normative) ASN.1 modules and W3C XSDs for an XMPP operational environment	112
E.1	Scope of Annex	112
E.2	ASN.1 modules for the XMPP operational environment	112
E.2.1	ASN.1 module for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	112
E.2.2	ASN.1 module for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	112
E.3	W3C XSDs for the XMPP operational environment	114
E.3.1	W3C XSD for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	114
E.3.2	W3C XSD for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	115
Annex F	(normative) Template for virtual API specifications	117
F.1	General	117
F.2	ASN.1 virtual API specification	118
F.3	ASN.1 virtual API specification for OSI environment	118
F.3.4	W3C XSD virtual API specification	118
Annex G	(normative) End-entity public-key certificate specification	120
G.1	Scope of annex	120
G.2	General requirement	120
G.3	Length considerations	120
G.4	Basic Structure requirement and recommendations	120

G.4.1	Version component	120
G.4.2	Serial number component	120
G.4.3	Issuer signature algorithm component	120
G.4.4	Issuer component	121
G.4.5	Validity component	121
G.4.6	Subject component	121
G.4.7	Subject public key Information component	121
G.4.8	Issuer unique ID and subject unique ID components	122
G.5	Extensions	122
G.5.1	General	122
G.5.2	Key usage extension	122
G.5.3	Revocation checking	122
G.5.4	IEC user role information extension	123
G.6	Specific requirements for operational environments	123
G.6.1	General	123
G.6.2	OSI operational environment	123
G.6.3	XMPP operational environment	123
Annex H (normative)	Lower layer requirements for the OSI operational environment	124
H.1	Scope of annex	124
H.2	Transport protocol class 0	124
H.2.1	Enforcement of maximum lengths	124
H.2.2	Response to Class 0 unsupported TPDU's	124
H.2.3	Transport selectors	124
H.3	IETF RFC 1006	125
H.3.1	General	125
H.3.2	Version number	125
H.3.3	Length	125
H.3.4	Keep-alive	125
Annex I (informative)	ASN.1 definition of ACSE	126
Bibliography	130
Figure 1	– Application and transport profiles (informative)	18
Figure 2	– T-profiles without and with TLS protection	24
Figure 3	– Association establishment	34
Figure 4	– Inclusion of User-data in SESSION DATA TRANSFER SPDU	36
Figure 5	– E2E security building blocks	43
Figure 6	– Relationship between environment, E2E-security and protected protocol	44
Figure 7	– Relationships between APDU's	44
Figure 8	– The scope of E2E-security specification	44
Figure 9	– Upper layer routing	73
Figure F.1	– Virtual API concept	117
Table 1	– Relationship between security and security measure combinations	19
Table 2	– Commented recommended cipher suites from IEC TS 62351-4:2007	26
Table 3	– Cipher suites combinations in the context of this document	27
Table 4	– Mapping of SecPDUs to ACSE-APDU's and EnvPDUs	69

Table 5 – Mapping of SecPDUs to XMPP stanzas	76
Table 6 – Conformance to operational environment	80
Table 7 – Conformance to modes of operation	80
Table 8 – Conformance to compatibility mode	80
Table 98 – Conformance to TLS cipher suites in compatibility mode	81
Table 119 – Conformance to mode of encryption	81
Table 10 – Conformance to native mode	81
Table 1210 – Conformance to TLS cipher suites in native mode	82
Table 1311 – Conformance to cryptographic algorithms for E2E-security	82
Table H.1 – TP class 0 maximum sizes	124

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**POWER SYSTEMS MANAGEMENT AND
ASSOCIATED INFORMATION EXCHANGE –
DATA AND COMMUNICATIONS SECURITY –****Part 4: Profiles including MMS and derivatives****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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62351-4 edition 1.1 contains the first edition (2018-11) [documents 57/2032/FDIS and 57/2053/RVD] and its amendment 1 (2020-07) [documents 57/2217/FDIS and 57/2053/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 62351-4 has been prepared by IEC technical committee 57: Power systems management and associated exchange.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in 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.

This IEC standard includes Code Components i.e. components that are intended to be directly processed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labelled in this standard as a Code Component.

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard to end users either directly or via distributors, subject to IEC software licensing conditions, which can be found at: www.iec.ch/CCv1.

In this document the following print types are used:

- Abstract Syntax Notation One (ASN.1) and W3C XML Schema Definition (W3C XSD) notions are presented in **Courier New** typeface; and
- when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in **Courier New** typeface.

A list of all parts in 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 the base publication and its amendment will remain unchanged until the stability 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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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

Part 4: Profiles including MMS and derivatives

1 Scope

1.1 General

This part of IEC 62351 extends the scope of IEC TS 62351-4:2007 [1]¹ by specifying a compatibility mode that provides interoperation with implementation based on IEC TS 62351-4:2007 and by specifying extended capabilities referred to as native mode.

This part of IEC 62351 specifies security requirements both at the transport layer and at the application layer. While IEC TS 62351-4:2007 primarily provided some limited support at the application layer for authentication during handshake for the Manufacturing Message Specification (MMS) based applications, this document also provides support for extended integrity and authentication both for the handshake phase and for the data transfer phase. It provides for shared key management and data transfer encryption at the application layer and it provides security end-to-end (E2E) with zero or more intermediate entities. While IEC TS 62351-4:2007 only provides support for systems based on the MMS, i.e. systems using an Open Systems Interworking (OSI) protocol stack, this document also provides support for application protocols using other protocol stacks, e.g. an Internet protocol suite (see 4.1). This support is extended to protect application protocols using XML encoding. This extended security at the application layer is referred to as E2E-security.

In addition to E2E security, this part of IEC 62351 also provides mapping to environmental protocols carrying the security related information. Only OSI and XMPP environments are currently considered.

It is intended that this part of IEC 62351 be referenced as a normative part of standards that have a need for using application protocols, e.g., MMS, in a secure manner.

It is anticipated that there are implementations, in particular Inter-Control Centre Communications Protocol (ICCP) implementations that are dependent on the IEC TS 62351-4:2007 specifications of the T-profile and the A-security-profile. The specifications from IEC TS 62351-4:2007 are therefore included in this part of IEC 62351. Implementations supporting these specifications will interwork with implementation based on IEC TS 62351-4:2007.

NOTE The A-security-profile is in the strict sense not a profile, but the term is here kept for historical reasons.

This document represents a set of mandatory and optional security specifications to be implemented to protect application protocols.

The initial audience for this document is the members of the working groups developing or making use of protocols. For the measures described in this part of IEC 62351 to take effect, they shall be accepted and referenced by the specifications for the protocols themselves.

The subsequent audience for this document is the developers of products that implement these protocols and the end user that want to specify requirements for its own environment.

¹ Numbers in square brackets refer to the bibliography.

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

1.2 Code components

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard to end users either directly or via distributors, subject to IEC software licensing conditions, which can be found at: www.iec.ch/CCv1.

The Code Components included in this IEC standard are also available as electronic machine readable file at: www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN.1_XSD.full.zip

In this document, code components are contained within Annexes A, B, C, D and E.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 TS 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 TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-3:2014/AMD1:2018

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

IEC 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 8073:1997 | Rec. ITU-T X.224 (1995), *Information technology – open systems interconnection – Protocol for providing the connection-mode transport service*

ISO/IEC 8823-1:1994 | Rec. ITU-T X.226 (1994), *Information technology – open systems interconnection – connection-oriented presentation protocol: Protocol specification*

ISO/IEC 8824-1 | Rec. ITU-T X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1 | Rec. ITU-T X.690, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8825-4 | Rec. ITU-T X.693, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

Rec. ITU-T X.227 (1995), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification*

NOTE 1 The corresponding International Standard ISO/IEC 8650-1:1996 has been withdrawn.

Rec. ITU-T X.227 (1995)/Amd.1 (1996), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification – Amendment 1: Incorporation of extensibility markers*

NOTE 2 The corresponding International Standard amendment ISO/IEC 8650-1:1996/Amd.1:1997 has been withdrawn.

IETF RFC 1006:1987, *ISO Transport Service on top of the TCP, Version: 3*

IETF RFC 2104:1997, *HMAC: Keyed-Hashing for Message Authentication*

IETF RFC 3526:2003, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*

IETF RFC 5114:2008, *Additional Diffie-Hellman Groups for Use with IETF Standards*

IETF RFC 5246:2008, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information*

IETF RFC 5639:2010, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*

IETF RFC 5869:2010, *HMAC-based Extract-and-Expand Key Derivation Function*

IETF RFC 6120:2011, *Extensible Messaging and Presence Protocol (XMPP): Core*

IETF RFC 6122:2011, *Extensible Messaging and Presence Protocol (XMPP): Address Format*