



IEC 62351-4

Edition 1.1 2020-07
CONSOLIDATED VERSION

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 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 interoperability 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*

SOMMAIRE

AVANT-PROPOS	138
1 Domaine d'application	140
1.1 Généralités	140
1.2 Composantes de code	141
2 Références normatives	141
3 Termes, définitions et termes abrégés	143
3.1 Généralités	143
3.2 Termes et définitions	143
3.3 Termes abrégés	147
4 Problèmes de sécurité couverts par la présente partie de l'IEC 62351	148
4.1 Modèles de référence pour la communication	148
4.2 Sécurité des profils application et transport.....	149
4.3 Mode compatible et mode natif	150
4.4 Menaces à la sécurité contrées.....	150
4.4.1 Généralités	150
4.4.2 Menaces contrées en mode compatible	150
4.4.3 Menaces contrées en mode natif	150
4.5 Méthodes d'attaque contrées	151
4.5.1 Généralités	151
4.5.2 Attaques contrées en mode compatible	151
4.5.3 Attaques contrées en mode natif.....	151
4.6 Journalisation	152
5 Exigences spécifiques	152
5.1 Exigences spécifiques concernant la pile communication ICCP/IEC 60870-6-x	152
5.2 Exigences spécifiques concernant l'IEC 61850	153
6 Sécurité de transport	153
6.1 Généralités	153
6.2 Application de la sécurité de couche de transport (TLS).....	153
6.2.1 Généralités	153
6.2.2 Concept de suite chiffrée TLS.....	154
6.2.3 Reprise de session TLS.....	154
6.2.4 Renégociation de session TLS.....	154
6.2.5 Nombre d'ancrages sécurisés pris en charge.....	154
6.2.6 Taille de certificat de clé publique.....	154
6.2.7 Période d'évaluation relative à l'état de révocation des certificats de clé publique	154
6.2.8 Validation de certificat de clé publique.....	155
6.2.9 Traitement des événements de sécurité.....	155
6.3 Sécurité de type T dans un environnement d'exploitation OSI	155
6.3.1 Généralités	155
6.3.2 Accès TCP	155
6.3.3 Désactivation de la TLS.....	156
6.3.4 Prise en charge des suites chiffrées TLS	156
6.4 Sécurité de type T dans un environnement d'exploitation XMPP	158
7 Vue d'ensemble concernant la sécurité de la couche application (informative).....	158

7.1	Généralités	158
7.2	Techniques de description	159
7.2.1	Généralités	159
7.2.2	ASN.1 en tant que définition de schéma XML	159
7.2.3	Définition de schéma W3C XML (W3C XSD).....	160
7.2.4	Espace de nommage XML	160
8	Utilisation d'algorithmes cryptographiques	160
8.1	Généralités	160
8.2	Définitions cryptographiques de base.....	160
8.3	Algorithmes de clé publique	161
8.4	Algorithmes de hachage.....	162
8.5	Algorithmes de signature	162
8.6	Algorithmes de chiffrement clés symétriques utilisés uniquement pour le chiffrement	162
8.7	Algorithmes de chiffrement authentifié	163
8.8	Algorithmes de valeur de vérification d'intégrité	164
9	Attribution d'identifiant d'objet (normatif)	164
10	Exigences générales relatives à la couche supérieure OSI (normatif)	164
10.1	Vue d'ensemble	164
10.2	Généralités concernant les exigences relatives à la couche supérieure OSI.....	166
10.3	Exigences relatives au protocole de session	166
10.4	Exigences relatives au protocole de présentation.....	166
10.4.1	Liste contextuelle.....	166
10.4.2	Syntaxes abstraites	167
10.4.3	Données d'utilisateur de présentation	167
10.4.4	Exigences relatives au codage ASN.1.....	168
10.5	Exigences relatives au protocole d'élément de service de contrôle d'association (ACSE)	168
10.5.1	Généralités	168
10.5.2	Version de protocole.....	168
10.5.3	Titres	168
10.5.4	Utilisation du type de donnée ASN.1 EXTERNAL.....	169
11	Profil de sécurité de type A (normatif).....	170
11.1	Exigences OSI spécifiques au profil de sécurité de type A	170
11.1.1	Généralités	170
11.1.2	Exigences supplémentaires relatives au protocole de session	170
11.1.3	Exigence supplémentaire relative au protocole de présentation	170
11.1.4	Exigences supplémentaires relatives à ACSE	171
11.2	Valeur d'authentification MMS.....	172
11.2.1	Généralités	172
11.2.2	Type de données de valeur d'authentification MMS	172
11.2.3	Traitement des demandes d'association (AARQ-apdu)	173
11.2.4	Traitement du résultat d'association (AARE-apdu)	174
12	Modèle de sécurité d'application bout-à-bout.....	174
12.1	Introduction et architecture générale	174
12.2	Spécifications relatives à la syntaxe abstraite	177
12.2.1	Généralités	177
13	Sécurité d'application bout-à-bout (normatif)	177
13.1	Gestion d'association.....	177

13.1.1	Concept général	177
13.1.2	Spécification relative au temps UTC	177
13.1.3	Demande d'établissement de liaison	178
13.1.4	Acceptation d'établissement de liaison	178
13.1.5	Rejet d'association par le protocole protégé	179
13.1.6	Rejet d'association dû à des questions de sécurité	179
13.1.7	Abandon d'établissement de liaison pour raison de sécurité	180
13.1.8	Abandon de transfert de données pour raison de sécurité.....	180
13.1.9	Abandon par protocole protégé.....	181
13.1.10	Demande de libération d'association	181
13.1.11	Réponse de libération d'association.....	182
13.2	Phase de transfert de données	182
13.2.1	Généralités.....	182
13.2.2	Transfert de données en clair	182
13.2.3	Transfert de données chiffrées	183
13.3	Types de données ClearToken.....	184
13.3.1	Le type de données ClearToken1	184
13.3.2	Le type de données ClearToken2	191
13.3.3	Le type de données ClearToken3	192
13.4	Spécifications d'authentification et d'intégrité.....	193
13.4.1	Le type de données Signature	193
13.4.2	Le type de données Authentificateur	193
14	Traitement des erreurs de sécurité E2E (normatif).....	194
14.1	Généralités	194
14.2	Spécification des diagnostics	194
14.2.1	Diagnostics d'établissement de liaison.....	194
14.2.2	Diagnostics de transfert de données.....	196
14.3	Vérification de la demande et de l'acceptation de l'établissement de liaison pour la sécurité E2E	197
14.3.1	Généralités.....	197
14.3.2	Vérification de signature	197
14.3.3	Vérification d'identité de protocole protégé	198
14.3.4	Vérification de ClearToken1.....	198
14.4	Vérification des informations de contrôle du protocole de sécurité lors du transfert de données	200
14.4.1	Généralités.....	200
14.4.2	Vérification de l'authentificateur.....	200
14.4.3	Vérifications de la valeur de ClearToken2.....	200
15	Sécurité E2E utilisée dans un environnement d'exploitation OSI.....	201
15.1	Généralités	201
15.2	Exigences supplémentaires relatives à la couche supérieure	201
15.2.1	Exigences supplémentaires relatives à la couche de présentation	201
15.2.2	Exigences supplémentaires relatives à l'ACSE	201
15.3	Gestion d'association dans un environnement d'exploitation OSI	202
15.3.1	Généralités.....	202
15.3.2	Mise en correspondance avec la demande d'association ACSE	202
15.3.3	Mise en correspondance avec la réponse d'association ACSE.....	203
15.3.4	Mise en correspondance avec l'abandon ACSE	203
15.3.5	Mise en correspondance avec la demande de libération ACSE	204

15.3.6	Mise en correspondance avec la réponse de libération ACSE.....	204
15.4	Transfert de données dans un environnement d'exploitation OSI	204
15.4.1	Généralités	204
15.4.2	Mise en correspondance de la SecPDU de transfert de données en clair.....	205
15.4.3	Mise en correspondance de la SecPDU de transfert de données chiffrées	205
15.5	Acheminement de la couche supérieure OSI.....	205
15.6	Vérifications relatives à un environnement d'exploitation OSI.....	207
15.6.1	Vérifications générales	207
15.6.2	Vérification de la mise en correspondance d'environnement	208
15.6.3	Diagnostics relatifs à un environnement d'exploitation OSI	208
16	Sécurité E2E utilisée dans un environnement d'exploitation XMPP.....	209
16.1	Généralités sur l'enveloppement à un environnement d'exploitation XMPP	209
16.2	Mise en correspondance des SecPDU avec les strophes iq	209
16.3	Mise en correspondance des SecPDU avec les strophes message	210
16.4	Traitement des erreurs de strophe XMPP.....	210
16.5	Espaces de nommage XML.....	211
16.6	Codage des EnvPDU dans les strophes XMPP	211
16.7	Associations multiples.....	212
16.8	Prise en considération des collisions de libération	212
17	Conformité au présent document	212
17.1	Généralités	212
17.2	Notation	212
17.3	Conformité à l'environnement d'exploitation	213
17.4	Conformité aux modes d'exploitation.....	213
17.5	Conformité au mode compatible.....	213
17.6	Conformité au mode natif.....	214
Annex A (normative)	Spécification ASN.1 officielle concernant le profil de sécurité de type A	217
Annex B (normative)	Spécification ASN.1 officielle concernant la sécurité E2E.....	218
Annex C (normative)	Spécification W3C XSD officielle concernant la sécurité E2E	229
Annex D (normative)	Module ASN.1 pour un environnement d'exploitation OSI.....	243
D.1	Domaine d'application de l'Annexe.....	243
D.2	Module ASN.1	243
Annex E (normative)	Modules ASN.1 et W3C XSD pour un environnement d'exploitation XMPP.....	245
E.1	Domaine d'application de l'Annexe.....	245
E.2	Modules ASN.1 pour l'environnement d'exploitation XMPP	245
E.2.1	Module ASN.1 pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas.....	245
E.2.2	Module ASN.1 pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	245
E.3	Modules W3C XSD pour l'environnement d'exploitation XMPP.....	247
E.3.1	W3C XSD pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas.....	247
E.3.2	W3C XSD pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	248
Annex F (normative)	Modèle pour spécifications relatives aux API virtuelles.....	250
F.1	Généralités	250

F.2	Spécification relative à l'API virtuelle ASN.1	251
F.3	Spécification relative à l'API virtuelle ASN.1 pour l'environnement OSI	251
F.3.4	Spécification relative à l'API virtuelle W3C XSD	252
Annex G	(normative) Spécification relative au certificat de clé publique d'entité finale	253
G.1	Domaine d'application de l'Annexe	253
G.2	Exigences générales	253
G.3	Considérations concernant la longueur	253
G.4	Exigences et recommandations relatives à la structure de base	253
G.4.1	Composante version	253
G.4.2	Composante numéro de série	253
G.4.3	Composante algorithme de signature de l'émetteur	254
G.4.4	Composante émetteur	254
G.4.5	Composante validité	254
G.4.6	Composante sujet	254
G.4.7	Composante information de clé publique sujet	254
G.4.8	Composantes Identifiant unique d'émetteur et Identifiant unique de sujet	255
G.5	Extensions	255
G.5.1	Généralités	255
G.5.2	Extension utilisation de clé	255
G.5.3	Vérification de révocation	255
G.5.4	Extension information concernant le rôle de l'utilisateur de l'IEC	256
G.6	Exigences spécifiques relatives aux environnements d'exploitation	256
G.6.1	Généralités	256
G.6.2	Environnement d'exploitation OSI	256
G.6.3	Environnement d'exploitation XMPP	256
Annex H	(normative) Exigences relatives à la couche inférieure dans un environnement d'exploitation OSI	257
H.1	Domaine d'application de l'Annexe	257
H.2	Protocole de transport de classe 0	257
H.2.1	Application des longueurs maximales	257
H.2.2	Réponse aux TPDU non pris en charge par la classe 0	257
H.2.3	Sélecteurs de transport	257
H.3	RFC 1006 de l'IETF	258
H.3.1	Généralités	258
H.3.2	Numéro de version	258
H.3.3	Longueur	258
H.3.4	Keepalive	258
Annex I	(informative) Définition ASN.1 de l'ACSE	259
Bibliographie	263
Figure 1	– Profils application et transport (informatif)	148
Figure 2	– Profils de type T sans et avec protection TLS	155
Figure 3	– Établissement d'association	165
Figure 4	– Inclusion des données utilisateur dans la SPDU SESSION DATA TRANSFER	168
Figure 5	– Blocs de construction de sécurité E2E	175
Figure 6	– Relation entre environnement, sécurité E2E et protocole protégé	175

Figure 7 – Relations entre APDU	176
Figure 8 – Domaine d'application de la spécification concernant la sécurité E2E	176
Figure 9 – Acheminement de la couche supérieure	206
Figure F.1 – Concept d'API virtuelle.....	250
Tableau 1 – Relation entre la sécurité et les combinaisons de mesures de sécurité	149
Tableau 2 - Suites chiffrées recommandées et commentées de l'IEC TS 62351-4:2007	157
Tableau 3 - Combinaisons de suites chiffrées dans le contexte du présent document	158
Tableau 4 – Mise en correspondance des SecPDU avec les APDU EnvPDU de l'ACSE	202
Tableau 5 – Mise en correspondance des SecPDU avec les strophes XMPP	209
Tableau 6 – Conformité à l'environnement d'exploitation	213
Tableau 7 – Conformité aux modes d'exploitation	213
Tableau 8 – Conformité au mode compatible
Tableau 98 – Conformité aux suites chiffrées TLS en mode compatible	214
Tableau 119 – Conformité aux modes de chiffrement.....	215
Tableau 10 – Conformité au mode natif.....
Tableau 1210 – Conformité aux suites chiffrées TLS en mode natif	215
Tableau 1311 – Conformité aux algorithmes cryptographiques pour la sécurité E2E	216
Tableau H.1 – Tailles maximales de protocole de transport de classe 0	257

COMMISSION ÉLECTRONIQUE INTERNATIONALE

**GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES
D'INFORMATIONS ASSOCIÉS –
SÉCURITÉ DES COMMUNICATIONS DES DONNÉES –****Partie 4: Profils comprenant le MMS et ses dérivés**

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

IEC 62351-4 édition 1.1 contient la première édition (2018-11) [documents 57/2032/FDIS et 57/2053/RVD] et son amendement 1 (2020-07) [documents 57/2217/FDIS et 57/2053/RVD].

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par l'amendement 1. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

La présente Norme internationale IEC 62351-4 a été établie par le Comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

La présente norme IEC comprend des Composantes de Code, c'est-à-dire des composantes conçues pour être directement traitées informatiquement. Ce contenu consiste en tout texte situé entre les marqueurs <DÉBUT DU CODE> et <FIN DU CODE>, ou sinon est clairement identifié dans la présente Norme comme étant une Composante de Code.

L'achat de la présente norme IEC comprend une licence de droit d'auteur permettant à l'acheteur de vendre du matériel logiciel contenant les composantes de code issues de la présente norme à des utilisateurs finaux, soit directement, soit par le l'intermédiaire de distributeurs, soumis aux conditions de licence de logiciels de l'IEC, qui peuvent être consultées à l'adresse: www.iec.ch/CCv1.

Dans le présent document, les caractères d'imprimerie suivants sont utilisés:

- les notions relatives à la Notation de Syntaxe Abstraite numéro un (ASN.1) et à la définition de schéma W3C XML (W3C XSD) sont présentées en police de caractères **Courier New**; et
- quand les types et les valeurs ASN.1 sont mentionnés dans le texte normal, ils se différencient de celui-ci en étant indiqués en police de caractères **Courier New**.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de son amendement ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS DES DONNÉES –

Partie 4: Profils comprenant le MMS et ses dérivés

1 Domaine d'application

1.1 Généralités

La présente partie de l'IEC 62351 étend le domaine d'application de l'IEC TS 62351-4:2007 [1]¹ en spécifiant un mode compatible qui assure une interopération avec une mise en œuvre fondée sur l'IEC TS 62351-4:2007 et en spécifiant les capacités étendues désignées comme mode natif.

La présente partie de l'IEC 62351 spécifie les exigences de sécurité concernant à la fois la couche transport et la couche application. Alors que l'IEC TS 62351-4:2007 apportait principalement une aide limitée concernant la couche application pour l'authentification lors de l'établissement de liaison des applications fondées sur la messagerie MMS (*manufacturing message specification*), le présent document fournit également une assistance quant à l'extension de l'intégrité et l'authentification lors des phases d'établissement de liaison et de transfert de données. Il pourvoit à la gestion essentielle partagée et au chiffrement de transfert de données pour la couche application et assure la sécurité bout-à-bout (E2E - *end-to-end*) avec zéro entité intermédiaire ou plus. Alors que l'IEC TS 62351-4:2007 apporte une assistance uniquement pour les systèmes fondés sur la MMS, c'est-à-dire les systèmes utilisant une pile de protocoles OSI (*open systems interworking* - interconnexion de systèmes ouverts), le présent document fournit également une assistance quant aux protocoles d'application utilisant d'autres piles de protocoles, par exemple une suite de protocoles Internet (voir 4.1). Cette assistance est étendue afin d'assurer la protection des protocoles d'application utilisant le codage XML. Cette sécurité étendue au niveau de la couche application est appelée sécurité E2E.

En plus de la sécurité E2E, la présente partie de l'IEC 62351 présente également la mise en correspondance avec les protocoles environnementaux comportant les informations concernant la sécurité. Seuls les environnements OSI et XMPP sont actuellement pris en considération.

Il est prévu que la présente partie de l'IEC 62351 soit référencée en tant que partie normative des normes qui ont un besoin d'utilisation des protocoles d'application, par exemple MMS, de façon sécurisée.

Il est escompté qu'il existe des mises en œuvre, notamment des mises en œuvre ICCP (*inter-control centre communications protocol* - protocole de communications inter-centres de conduite) qui dépendent des spécifications de l'IEC TS 62351-4:2007 du profil T et du profil de sécurité de type A. Par conséquent, les spécifications issues de l'IEC 62351-4:2007 sont incluses dans la présente partie de l'IEC 62351. Les mises en œuvre appuyant ces spécifications interagissent avec la mise en œuvre fondée sur l'IEC TS 62351-4:2007.

NOTE Le profil de sécurité de type A n'est pas un profil au sens strict du terme, mais ce terme est conservé ici pour des raisons historiques.

¹ Les chiffres entre crochets se réfèrent à la bibliographie.

Le présent document constitue un ensemble de spécifications obligatoires et facultatives relatives à la sécurité qui doivent être mises en œuvre afin d'assurer la protection des protocoles d'application.

Le public initial auquel ce document est destiné est constitué des membres des groupes de travail développant ou utilisant des protocoles. Pour prendre effet, les mesures décrites dans la présente partie de l'IEC 62351 doivent être acceptées et référencées par les spécifications pour les protocoles eux-mêmes.

Les autres utilisateurs auxquels s'adresse le présent document sont les concepteurs de produits appliquant ces protocoles et les utilisateurs finaux qui veulent spécifier des exigences quant à leur propre environnement

Des parties du présent document peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

1.2 Composantes de code

L'achat de la présente norme IEC comprend une licence de droit d'auteur permettant à l'acheteur de vendre du matériel logiciel contenant les composantes de code issues de la présente norme à des utilisateurs finaux, soit directement, soit par l'intermédiaire de distributeurs, soumis aux conditions de licence de logiciels de l'IEC, qui peuvent être consultées à l'adresse: www.iec.ch/CCv1.

Les Composantes de Code comprises dans la présente norme IEC sont également disponibles sous forme de fichier électronique lisible par machine à l'adresse: www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN.1_XSD.full.zip

Dans le présent document, les composantes de code sont comprises dans les Annexes A, B, C, D et E.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris d'éventuels amendements).

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* (disponible en anglais seulement)

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3:2014, *Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 3: Sécurité des réseaux et des systèmes de communication - Profils comprenant 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* (disponible en anglais seulement)

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* (disponible en anglais seulement)

ISO/IEC 8073:1997 | Rec. UIT-T X.224 (1995), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole assurant le service de transport en mode connexion*

ISO/IEC 8823-1:1994 | Rec. UIT-T X.226 (1994), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole de présentation en mode connexion: Spécification du protocole*

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

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

ISO/IEC 8825-4 | Rec. UIT-T X.693, *Technologies de l'information – Règles de codage ASN.1: Règles de codage XML étendues (XER)*

ISO 8601:2004, *Éléments de données et formats d'échange – Échange d'information – Représentation de la date et de l'heure*

ISO 9506-2:2003, *Systèmes d'automatisation industrielle – Spécification de messagerie industrielle – Partie 2: Spécification de protocole*

ISO/IEC 9594-8:2020 | Rec. UIT-T X.509 (2019), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: Cadre général des certificats de clé publique et d'attribut*

Rec. UIT-T X.227 (1995), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole*

NOTE 1 La Norme internationale correspondante ISO/IEC 8650-1:1996 a été supprimée.

Rec. UIT-T X.227(1995)/Amd.1 (1996), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole – Amendement 1: Incorporation de marqueurs d'extensibilité*

NOTE 2 La Norme internationale correspondante 8650 ISO/IEC 8650: -1/ Amd.1:1997 a été supprimée.

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*

FINAL VERSION

VERSION FINALE

**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.....	30
8.5	Signature algorithms.....	30
8.6	Symmetric key algorithms	31
8.7	Authenticated encryption algorithms	31
8.8	Integrity check value algorithms.....	32
9	Object identifier allocation (normative).....	32
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.....	34
10.4.1	Context list	34
10.4.2	Abstract syntaxes	35
10.4.3	Presentation user data.....	35
10.4.4	ASN.1 encoding requirements	36
10.5	Association control service element (ACSE) protocol requirements.....	36
10.5.1	General	36
10.5.2	Protocol version.....	36
10.5.3	Titles	36
10.5.4	Use of ASN.1 EXTERNAL data type	37
11	A-security profile (normative).....	37
11.1	OSI requirements specific to A-security profile	37
11.1.1	General	37
11.1.2	Additional session protocol requirements.....	38
11.1.3	Additional presentation protocol requirement	38
11.1.4	Additional ACSE requirements.....	38
11.2	MMS Authentication value.....	39
11.2.1	General	39
11.2.2	MMS-Authentication value data type.....	40
11.2.3	Handling of the association request (AARQ-apdu)	40
11.2.4	Handling of the association result (AARE-apdu).....	41
12	End-to-end application security model	41
12.1	Introduction and general architecture	41
12.2	Abstract syntax specifications	43
12.2.1	General	43
13	End-to-end application security (normative).....	44
13.1	Association management	44
13.1.1	General concept	44
13.1.2	UTC time specification.....	44
13.1.3	Handshake request.....	44

13.1.4	Handshake accept	45
13.1.5	Association reject by the protected protocol	46
13.1.6	Association reject due to security issues	46
13.1.7	Handshake security abort	47
13.1.8	Data transfer security abort	47
13.1.9	Abort by protected protocol	47
13.1.10	Association release request	48
13.1.11	Association release response	48
13.2	Data transfer phase	49
13.2.1	General	49
13.2.2	Clear data transfer	49
13.2.3	Encrypted data transfer	49
13.3	ClearToken data types	50
13.3.1	The ClearToken1 data type	50
13.3.2	The ClearToken2 data type	55
13.3.3	The ClearToken3 data type	56
13.4	Authentication and integrity specifications	57
13.4.1	The Signature data type	57
13.4.2	The authenticator data type	57
14	E2E security error handling (normative)	57
14.1	General	57
14.2	Specification of diagnostics	57
14.2.1	Handshake diagnostics	57
14.2.2	The data transfer diagnostics	59
14.3	Checking of E2E-security handshake request and accept	60
14.3.1	General	60
14.3.2	Signature checking	60
14.3.3	Protected protocol identity checking	61
14.3.4	ClearToken1 checking	61
14.4	Checking of security protocol control information during data transfer	63
14.4.1	General	63
14.4.2	Authenticator checking	63
14.4.3	Checks of the ClearToken2 value	63
15	E2E security used in an OSI operational environment	64
15.1	General	64
15.2	Additional upper layer requirements	64
15.2.1	Additional presentation layer requirements	64
15.2.2	Additional ACSE requirements	64
15.3	Association management in an OSI operational environment	64
15.3.1	General	64
15.3.2	Mapping to ACSE association request	65
15.3.3	Mapping to ACSE association response	65
15.3.4	Mapping to ACSE abort	66
15.3.5	Mapping to ACSE release request	67
15.3.6	Mapping to ACSE release response	67
15.4	Data transfer in OSI operational environment	67
15.4.1	General	67
15.4.2	Mapping of the clear data transfer SecPDU	67
15.4.3	Mapping of the encrypted data transfer SecPDU	68

15.5	OSI upper layer routing	68
15.6	OSI operational environment checking	70
15.6.1	General checking	70
15.6.2	Environment mapping checking	70
15.6.3	OSI operational environment diagnostics	71
16	E2E security used in in an XMPP operational environment	71
16.1	General on wrapping to an XMPP operational environment	71
16.2	Mapping of SecPDUs to iq stanzas	72
16.3	Mapping of SecPDUs to message stanzas	73
16.4	XMPP stanza error handling	73
16.5	XML namespaces	74
16.6	Encoding of EnvPDUs within XMPP stanzas	74
16.7	Multiple associations	75
16.8	Release collision consideration	75
17	Conformance to this document	75
17.1	General	75
17.2	Notation	75
17.3	Conformance to operational environment	75
17.4	Conformance to modes of operation	76
17.5	Conformance to compatibility mode	76
17.6	Conformance to native mode	76
Annex A	(normative) Formal ASN.1 specification for the A-security-profile	79
Annex B	(normative) Formal ASN.1 specification for the End-to-End security	80
Annex C	(normative) Formal W3C XSD specification for the end-to-end security	85
Annex D	(normative) ASN.1 module for OSI operational environment	93
D.1	Scope of annex	93
D.2	ASN.1 module	93
Annex E	(normative) ASN.1 modules and W3C XSDs for an XMPP operational environment	95
E.1	Scope of Annex	95
E.2	ASN.1 modules for the XMPP operational environment	95
E.2.1	ASN.1 module for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	95
E.2.2	ASN.1 module for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	95
E.3	W3C XSDs for the XMPP operational environment	97
E.3.1	W3C XSD for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	97
E.3.2	W3C XSD for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	98
Annex F	(normative) Template for virtual API specifications	100
F.1	General	100
F.2	ASN.1 virtual API specification	101
F.3	ASN.1 virtual API specification for OSI environment	101
F.4	W3C XSD virtual API specification	101
Annex G	(normative) End-entity public-key certificate specification	103
G.1	Scope of annex	103
G.2	General requirement	103
G.3	Length considerations	103
G.4	Basic Structure requirement and recommendations	103

G.4.1	Version component	103
G.4.2	Serial number component	103
G.4.3	Issuer signature algorithm component	103
G.4.4	Issuer component	104
G.4.5	Validity component	104
G.4.6	Subject component	104
G.4.7	Subject public key Information component	104
G.4.8	Issuer unique ID and subject unique ID components	105
G.5	Extensions	105
G.5.1	General	105
G.5.2	Key usage extension	105
G.5.3	Revocation checking	105
G.5.4	IEC user role information extension	106
G.6	Specific requirements for operational environments	106
G.6.1	General	106
G.6.2	OSI operational environment	106
G.6.3	XMPP operational environment	106
Annex H (normative)	Lower layer requirements for the OSI operational environment	107
H.1	Scope of annex	107
H.2	Transport protocol class 0	107
H.2.1	Enforcement of maximum lengths	107
H.2.2	Response to Class 0 unsupported TPDU's	107
H.2.3	Transport selectors	107
H.3	IETF RFC 1006	108
H.3.1	General	108
H.3.2	Version number	108
H.3.3	Length	108
H.3.4	Keep-alive	108
Annex I (informative)	ASN.1 definition of ACSE	109
Bibliography	113
Figure 1	– Application and transport profiles (informative)	18
Figure 2	– T-profiles without and with TLS protection	24
Figure 3	– Association establishment	33
Figure 4	– Inclusion of User-data in SESSION DATA TRANSFER SPDU	36
Figure 5	– E2E security building blocks	42
Figure 6	– Relationship between environment, E2E-security and protected protocol	42
Figure 7	– Relationships between APDU's	43
Figure 8	– The scope of E2E-security specification	43
Figure 9	– Upper layer routing	69
Figure F.1	– Virtual API concept	100
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 EnvPDUs	65

Table 5 – Mapping of SecPDUs to XMPP stanzas	72
Table 6 – Conformance to operational environment	76
Table 7 – Conformance to modes of operation	76
Table 8 – Conformance to TLS cipher suites in compatibility mode	76
Table 9 – Conformance to mode of encryption	77
Table 10 – Conformance to TLS cipher suites in native mode	77
Table 11 – Conformance to cryptographic algorithms for E2E-security	78
Table H.1 – TP class 0 maximum sizes	107

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].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted 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 interoperability 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*

SOMMAIRE

AVANT-PROPOS	122
1 Domaine d'application	124
1.1 Généralités	124
1.2 Composantes de code	125
2 Références normatives	125
3 Termes, définitions et termes abrégés	127
3.1 Généralités	127
3.2 Termes et définitions	127
3.3 Termes abrégés	131
4 Problèmes de sécurité couverts par la présente partie de l'IEC 62351	132
4.1 Modèles de référence pour la communication	132
4.2 Sécurité des profils application et transport.....	133
4.3 Mode compatible et mode natif	134
4.4 Menaces à la sécurité contrées.....	134
4.4.1 Généralités	134
4.4.2 Menaces contrées en mode compatible	134
4.4.3 Menaces contrées en mode natif	134
4.5 Méthodes d'attaque contrées	135
4.5.1 Généralités	135
4.5.2 Attaques contrées en mode compatible	135
4.5.3 Attaques contrées en mode natif.....	135
4.6 Journalisation	136
5 Exigences spécifiques	136
5.1 Exigences spécifiques concernant la pile communication ICCP/IEC 60870-6-x	136
5.2 Exigences spécifiques concernant l'IEC 61850	137
6 Sécurité de transport	137
6.1 Généralités	137
6.2 Application de la sécurité de couche de transport (TLS).....	137
6.2.1 Généralités	137
6.2.2 Concept de suite chiffrée TLS.....	138
6.2.3 Reprise de session TLS.....	138
6.2.4 Renégociation de session TLS.....	138
6.2.5 Nombre d'ancrages sécurisés pris en charge.....	138
6.2.6 Taille de certificat de clé publique.....	138
6.2.7 Période d'évaluation relative à l'état de révocation des certificats de clé publique	138
6.2.8 Validation de certificat de clé publique.....	139
6.2.9 Traitement des événements de sécurité.....	139
6.3 Sécurité de type T dans un environnement d'exploitation OSI	139
6.3.1 Généralités	139
6.3.2 Accès TCP	139
6.3.3 Désactivation de la TLS.....	140
6.3.4 Prise en charge des suites chiffrées TLS	140
6.4 Sécurité de type T dans un environnement d'exploitation XMPP	142
7 Vue d'ensemble concernant la sécurité de la couche application (informative).....	142

7.1	Généralités	142
7.2	Techniques de description	143
7.2.1	Généralités	143
7.2.2	ASN.1 en tant que définition de schéma XML	143
7.2.3	Définition de schéma W3C XML (W3C XSD).....	144
7.2.4	Espace de nommage XML	144
8	Utilisation d'algorithmes cryptographiques	144
8.1	Généralités	144
8.2	Définitions cryptographiques de base.....	144
8.3	Algorithmes de clé publique	145
8.4	Algorithmes de hachage.....	146
8.5	Algorithmes de signature	146
8.6	Algorithmes de clés symétriques	146
8.7	Algorithmes de chiffrement authentifié	147
8.8	Algorithmes de valeur de vérification d'intégrité	147
9	Attribution d'identifiant d'objet (normatif)	148
10	Exigences générales relatives à la couche supérieure OSI (normatif)	148
10.1	Vue d'ensemble	148
10.2	Généralités concernant les exigences relatives à la couche supérieure OSI.....	149
10.3	Exigences relatives au protocole de session	149
10.4	Exigences relatives au protocole de présentation.....	150
10.4.1	Liste contextuelle.....	150
10.4.2	Syntaxes abstraites	150
10.4.3	Données d'utilisateur de présentation	151
10.4.4	Exigences relatives au codage ASN.1.....	152
10.5	Exigences relatives au protocole d'élément de service de contrôle d'association (ACSE)	152
10.5.1	Généralités	152
10.5.2	Version de protocole.....	152
10.5.3	Titres	152
10.5.4	Utilisation du type de donnée ASN.1 EXTERNAL.....	153
11	Profil de sécurité de type A (normatif).....	153
11.1	Exigences OSI spécifiques au profil de sécurité de type A	153
11.1.1	Généralités	153
11.1.2	Exigences supplémentaires relatives au protocole de session	153
11.1.3	Exigence supplémentaire relative au protocole de présentation	154
11.1.4	Exigences supplémentaires relatives à ACSE	154
11.2	Valeur d'authentification MMS.....	155
11.2.1	Généralités	155
11.2.2	Type de données de valeur d'authentification MMS	155
11.2.3	Traitement des demandes d'association (AARQ-apdu)	156
11.2.4	Traitement du résultat d'association (AARE-apdu)	157
12	Modèle de sécurité d'application bout-à-bout.....	157
12.1	Introduction et architecture générale	157
12.2	Spécifications relatives à la syntaxe abstraite	159
12.2.1	Généralités	159
13	Sécurité d'application bout-à-bout (normatif)	160
13.1	Gestion d'association.....	160

13.1.1	Concept général	160
13.1.2	Spécification relative au temps UTC	160
13.1.3	Demande d'établissement de liaison	160
13.1.4	Acceptation d'établissement de liaison	161
13.1.5	Rejet d'association par le protocole protégé	162
13.1.6	Rejet d'association dû à des questions de sécurité	162
13.1.7	Abandon d'établissement de liaison pour raison de sécurité	163
13.1.8	Abandon de transfert de données pour raison de sécurité.....	163
13.1.9	Abandon par protocole protégé.....	164
13.1.10	Demande de libération d'association	164
13.1.11	Réponse de libération d'association.....	165
13.2	Phase de transfert de données	165
13.2.1	Généralités	165
13.2.2	Transfert de données en clair	165
13.2.3	Transfert de données chiffrées	165
13.3	Types de données ClearToken.....	166
13.3.1	Le type de données ClearToken1	166
13.3.2	Le type de données ClearToken2	172
13.3.3	Le type de données ClearToken3	173
13.4	Spécifications d'authentification et d'intégrité.....	174
13.4.1	Le type de données Signature	174
13.4.2	Le type de données Authentificateur	174
14	Traitement des erreurs de sécurité E2E (normatif).....	174
14.1	Généralités	174
14.2	Spécification des diagnostics	174
14.2.1	Diagnostics d'établissement de liaison.....	174
14.2.2	Diagnostics de transfert de données.....	176
14.3	Vérification de la demande et de l'acceptation de l'établissement de liaison pour la sécurité E2E	177
14.3.1	Généralités	177
14.3.2	Vérification de signature	178
14.3.3	Vérification d'identité de protocole protégé	178
14.3.4	Vérification de ClearToken1.....	178
14.4	Vérification des informations de contrôle du protocole de sécurité lors du transfert de données	180
14.4.1	Généralités	180
14.4.2	Vérification de l'authentificateur.....	180
14.4.3	Vérifications de la valeur de ClearToken2.....	181
15	Sécurité E2E utilisée dans un environnement d'exploitation OSI.....	181
15.1	Généralités	181
15.2	Exigences supplémentaires relatives à la couche supérieure	181
15.2.1	Exigences supplémentaires relatives à la couche de présentation	181
15.2.2	Exigences supplémentaires relatives à l'ACSE	181
15.3	Gestion d'association dans un environnement d'exploitation OSI	182
15.3.1	Généralités	182
15.3.2	Mise en correspondance avec la demande d'association ACSE	183
15.3.3	Mise en correspondance avec la réponse d'association ACSE.....	183
15.3.4	Mise en correspondance avec l'abandon ACSE	184
15.3.5	Mise en correspondance avec la demande de libération ACSE	184

15.3.6	Mise en correspondance avec la réponse de libération ACSE.....	185
15.4	Transfert de données dans un environnement d'exploitation OSI	185
15.4.1	Généralités	185
15.4.2	Mise en correspondance de la SecPDU de transfert de données en clair.....	185
15.4.3	Mise en correspondance de la SecPDU de transfert de données chiffrées	185
15.5	Acheminement de la couche supérieure OSI.....	186
15.6	Vérifications relatives à un environnement d'exploitation OSI.....	187
15.6.1	Vérifications générales	187
15.6.2	Vérification de la mise en correspondance d'environnement	188
15.6.3	Diagnostics relatifs à un environnement d'exploitation OSI	188
16	Sécurité E2E utilisée dans un environnement d'exploitation XMPP.....	189
16.1	Généralités sur l'enveloppement à un environnement d'exploitation XMPP	189
16.2	Mise en correspondance des SecPDU avec les strophes iq	189
16.3	Mise en correspondance des SecPDU avec les strophes message	190
16.4	Traitement des erreurs de strophe XMPP.....	190
16.5	Espaces de nommage XML.....	191
16.6	Codage des EnvPDU dans les strophes XMPP	191
16.7	Associations multiples.....	192
16.8	Prise en considération des collisions de libération	192
17	Conformité au présent document	192
17.1	Généralités	192
17.2	Notation	192
17.3	Conformité à l'environnement d'exploitation	193
17.4	Conformité aux modes d'exploitation.....	193
17.5	Conformité au mode compatible.....	193
17.6	Conformité au mode natif.....	194
Annex A (normative)	Spécification ASN.1 officielle concernant le profil de sécurité de type A	196
Annex B (normative)	Spécification ASN.1 officielle concernant la sécurité E2E.....	197
Annex C (normative)	Spécification W3C XSD officielle concernant la sécurité E2E	202
Annex D (normative)	Module ASN.1 pour un environnement d'exploitation OSI.....	209
D.1	Domaine d'application de l'Annexe.....	209
D.2	Module ASN.1	209
Annex E (normative)	Modules ASN.1 et W3C XSD pour un environnement d'exploitation XMPP.....	211
E.1	Domaine d'application de l'Annexe.....	211
E.2	Modules ASN.1 pour l'environnement d'exploitation XMPP	211
E.2.1	Module ASN.1 pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas.....	211
E.2.2	Module ASN.1 pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	211
E.3	Modules W3C XSD pour l'environnement d'exploitation XMPP.....	213
E.3.1	W3C XSD pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas.....	213
E.3.2	W3C XSD pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	214
Annex F (normative)	Modèle pour spécifications relatives aux API virtuelles.....	216
F.1	Généralités	216

F.2	Spécification relative à l'API virtuelle ASN.1	217
F.3	Spécification relative à l'API virtuelle ASN.1 pour l'environnement OSI	217
F.4	Spécification relative à l'API virtuelle W3C XSD	218
Annex G	(normative) Spécification relative au certificat de clé publique d'entité finale	219
G.1	Domaine d'application de l'Annexe	219
G.2	Exigences générales	219
G.3	Considérations concernant la longueur	219
G.4	Exigences et recommandations relatives à la structure de base	219
G.4.1	Composante version	219
G.4.2	Composante numéro de série	219
G.4.3	Composante algorithme de signature de l'émetteur	220
G.4.4	Composante émetteur	220
G.4.5	Composante validité	220
G.4.6	Composante sujet	220
G.4.7	Composante information de clé publique sujet	220
G.4.8	Composantes Identifiant unique d'émetteur et Identifiant unique de sujet	221
G.5	Extensions	221
G.5.1	Généralités	221
G.5.2	Extension utilisation de clé	221
G.5.3	Vérification de révocation	221
G.5.4	Extension information concernant le rôle de l'utilisateur de l'IEC	222
G.6	Exigences spécifiques relatives aux environnements d'exploitation	222
G.6.1	Généralités	222
G.6.2	Environnement d'exploitation OSI	222
G.6.3	Environnement d'exploitation XMPP	222
Annex H	(normative) Exigences relatives à la couche inférieure dans un environnement d'exploitation OSI	223
H.1	Domaine d'application de l'Annexe	223
H.2	Protocole de transport de classe 0	223
H.2.1	Application des longueurs maximales	223
H.2.2	Réponse aux TPDU non pris en charge par la classe 0	223
H.2.3	Sélecteurs de transport	223
H.3	RFC 1006 de l'IETF	224
H.3.1	Généralités	224
H.3.2	Numéro de version	224
H.3.3	Longueur	224
H.3.4	Keepalive	224
Annex I	(informative) Définition ASN.1 de l'ACSE	225
Bibliographie	229
Figure 1	– Profils application et transport (informatif)	132
Figure 2	– Profils de type T sans et avec protection TLS	139
Figure 3	– Établissement d'association	149
Figure 4	– Inclusion des données utilisateur dans la SPDU SESSION DATA TRANSFER	151
Figure 5	– Blocs de construction de sécurité E2E	158
Figure 6	– Relation entre environnement, sécurité E2E et protocole protégé	158

Figure 7 – Relations entre APDU	158
Figure 8 – Domaine d’application de la spécification concernant la sécurité E2E	159
Figure 9 – Acheminement de la couche supérieure	186
Figure F.1 – Concept d’API virtuelle.....	216
Tableau 1 – Relation entre la sécurité et les combinaisons de mesures de sécurité	133
Tableau 2 - Suites chiffrées recommandées et commentées de l’IEC TS 62351-4:2007	141
Tableau 3 - Combinaisons de suites chiffrées dans le contexte du présent document	142
Tableau 4 – Mise en correspondance des SecPDU avec les EnvPDU de l’ACSE	183
Tableau 5 – Mise en correspondance des SecPDU avec les strophes XMPP	189
Tableau 6 – Conformité à l’environnement d’exploitation	193
Tableau 7 – Conformité aux modes d’exploitation	193
Tableau 8 – Conformité aux suites chiffrées TLS en mode compatible	194
Tableau 9 – Conformité aux modes de chiffrement.....	194
Tableau 10 – Conformité aux suites chiffrées TLS en mode natif	194
Tableau 11 – Conformité aux algorithmes cryptographiques pour la sécurité E2E	195
Tableau H.1 – Tailles maximales de protocole de transport de classe 0	223

COMMISSION ÉLECTRONIQUE INTERNATIONALE

**GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES
D'INFORMATIONS ASSOCIÉS –
SÉCURITÉ DES COMMUNICATIONS DES DONNÉES –****Partie 4: Profils comprenant le MMS et ses dérivés**

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

IEC 62351-4 édition 1.1 contient la première édition (2018-11) [documents 57/2032/FDIS et 57/2053/RVD] et son amendement 1 (2020-07) [documents 57/2217/FDIS et 57/2053/RVD].

Cette version Finale ne montre pas les modifications apportées au contenu technique par l'amendement 1. Une version Redline montrant toutes les modifications est disponible dans cette publication.

La présente Norme internationale IEC 62351-4 a été établie par le Comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

La présente norme IEC comprend des Composantes de Code, c'est-à-dire des composantes conçues pour être directement traitées informatiquement. Ce contenu consiste en tout texte situé entre les marqueurs <DÉBUT DU CODE> et <FIN DU CODE>, ou sinon est clairement identifié dans la présente Norme comme étant une Composante de Code.

L'achat de la présente norme IEC comprend une licence de droit d'auteur permettant à l'acheteur de vendre du matériel logiciel contenant les composantes de code issues de la présente norme à des utilisateurs finaux, soit directement, soit par le l'intermédiaire de distributeurs, soumis aux conditions de licence de logiciels de l'IEC, qui peuvent être consultées à l'adresse: www.iec.ch/CCv1.

Dans le présent document, les caractères d'imprimerie suivants sont utilisés:

- les notions relatives à la Notation de Syntaxe Abstraite numéro un (ASN.1) et à la définition de schéma W3C XML (W3C XSD) sont présentées en police de caractères **Courier New**; et
- quand les types et les valeurs ASN.1 sont mentionnés dans le texte normal, ils se différencient de celui-ci en étant indiqués en police de caractères **Courier New**.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de son amendement ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

<p>IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.</p>
--

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS DES DONNÉES –

Partie 4: Profils comprenant le MMS et ses dérivés

1 Domaine d'application

1.1 Généralités

La présente partie de l'IEC 62351 étend le domaine d'application de l'IEC TS 62351-4:2007 [1]¹ en spécifiant un mode compatible qui assure une interopération avec une mise en œuvre fondée sur l'IEC TS 62351-4:2007 et en spécifiant les capacités étendues désignées comme mode natif.

La présente partie de l'IEC 62351 spécifie les exigences de sécurité concernant à la fois la couche transport et la couche application. Alors que l'IEC TS 62351-4:2007 apportait principalement une aide limitée concernant la couche application pour l'authentification lors de l'établissement de liaison des applications fondées sur la messagerie MMS (*manufacturing message specification*), le présent document fournit également une assistance quant à l'extension de l'intégrité et l'authentification lors des phases d'établissement de liaison et de transfert de données. Il pourvoit à la gestion essentielle partagée et au chiffrement de transfert de données pour la couche application et assure la sécurité bout-à-bout (E2E - *end-to-end*) avec zéro entité intermédiaire ou plus. Alors que l'IEC TS 62351-4:2007 apporte une assistance uniquement pour les systèmes fondés sur la MMS, c'est-à-dire les systèmes utilisant une pile de protocoles OSI (*open systems interworking* - interconnexion de systèmes ouverts), le présent document fournit également une assistance quant aux protocoles d'application utilisant d'autres piles de protocoles, par exemple une suite de protocoles Internet (voir 4.1). Cette assistance est étendue afin d'assurer la protection des protocoles d'application utilisant le codage XML. Cette sécurité étendue au niveau de la couche application est appelée sécurité E2E.

En plus de la sécurité E2E, la présente partie de l'IEC 62351 présente également la mise en correspondance avec les protocoles environnementaux comportant les informations concernant la sécurité. Seuls les environnements OSI et XMPP sont actuellement pris en considération.

Il est prévu que la présente partie de l'IEC 62351 soit référencée en tant que partie normative des normes qui ont un besoin d'utilisation des protocoles d'application, par exemple MMS, de façon sécurisée.

Il est escompté qu'il existe des mises en œuvre, notamment des mises en œuvre ICCP (*inter-control centre communications protocol* - protocole de communications inter-centres de conduite) qui dépendent des spécifications de l'IEC TS 62351-4:2007 du profil T et du profil de sécurité de type A. Par conséquent, les spécifications issues de l'IEC 62351-4:2007 sont incluses dans la présente partie de l'IEC 62351. Les mises en œuvre appuyant ces spécifications interagissent avec la mise en œuvre fondée sur l'IEC TS 62351-4:2007.

NOTE Le profil de sécurité de type A n'est pas un profil au sens strict du terme, mais ce terme est conservé ici pour des raisons historiques.

¹ Les chiffres entre crochets se réfèrent à la bibliographie.

Le présent document constitue un ensemble de spécifications obligatoires et facultatives relatives à la sécurité qui doivent être mises en œuvre afin d'assurer la protection des protocoles d'application.

Le public initial auquel ce document est destiné est constitué des membres des groupes de travail développant ou utilisant des protocoles. Pour prendre effet, les mesures décrites dans la présente partie de l'IEC 62351 doivent être acceptées et référencées par les spécifications pour les protocoles eux-mêmes.

Les autres utilisateurs auxquels s'adresse le présent document sont les concepteurs de produits appliquant ces protocoles et les utilisateurs finaux qui veulent spécifier des exigences quant à leur propre environnement

Des parties du présent document peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

1.2 Composantes de code

L'achat de la présente norme IEC comprend une licence de droit d'auteur permettant à l'acheteur de vendre du matériel logiciel contenant les composantes de code issues de la présente norme à des utilisateurs finaux, soit directement, soit par l'intermédiaire de distributeurs, soumis aux conditions de licence de logiciels de l'IEC, qui peuvent être consultées à l'adresse: www.iec.ch/CCv1.

Les Composantes de Code comprises dans la présente norme IEC sont également disponibles sous forme de fichier électronique lisible par machine à l'adresse: www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN.1_XSD.full.zip

Dans le présent document, les composantes de code sont comprises dans les Annexes A, B, C, D et E.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris d'éventuels amendements).

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* (disponible en anglais seulement)

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3:2014, *Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 3: Sécurité des réseaux et des systèmes de communication - Profils comprenant 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* (disponible en anglais seulement)

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* (disponible en anglais seulement)

ISO/IEC 8073:1997 | Rec. UIT-T X.224 (1995), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole assurant le service de transport en mode connexion*

ISO/IEC 8823-1:1994 | Rec. UIT-T X.226 (1994), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole de présentation en mode connexion: Spécification du protocole*

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

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

ISO/IEC 8825-4 | Rec. UIT-T X.693, *Technologies de l'information – Règles de codage ASN.1: Règles de codage XML étendues (XER)*

ISO 8601:2004, *Éléments de données et formats d'échange – Échange d'information – Représentation de la date et de l'heure*

ISO 9506-2:2003, *Systèmes d'automatisation industrielle – Spécification de messagerie industrielle – Partie 2: Spécification de protocole*

ISO/IEC 9594-8:2020 | Rec. UIT-T X.509 (2019), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: Cadre général des certificats de clé publique et d'attribut*

Rec. UIT-T X.227 (1995), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole*

NOTE 1 La Norme internationale correspondante ISO/IEC 8650-1:1996 a été supprimée.

Rec. UIT-T X.227(1995)/Amd.1 (1996), *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole – Amendement 1: Incorporation de marqueurs d'extensibilité*

NOTE 2 La Norme internationale correspondante 8650 ISO/IEC 8650: -1/ Amd.1:1997 a été supprimée.

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*