



IEC 62351-4

Edition 1.0 2018-11

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 978-2-8322-7714-0

**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.**

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	17
4.1 Communications reference models	17
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	26
7 Application layer security overview (informative).....	26
7.1 General.....	26
7.2 Description techniques.....	27

7.2.1	General	27
7.2.2	ASN.1 as an XML schema definition	27
7.2.3	W3C XML Schema Definition (W3C XSD)	28
7.2.4	XML namespace	28
8	Use of cryptographic algorithms	28
8.1	General.....	28
8.2	Basic cryptographic definitions.....	28
8.3	Public-key algorithms.....	29
8.4	Hash algorithms	30
8.5	Signature algorithms	30
8.6	Symmetric encryption algorithms used for encryption only	30
8.7	Authenticated encryption algorithms	31
8.8	Integrity check value algorithms	31
9	Object identifier allocation (normative).....	32
10	General OSI upper layer requirements (normative).....	32
10.1	Overview.....	32
10.2	General on OSI upper layer requirements	33
10.3	Session protocol requirements	33
10.4	Presentation protocol requirements.....	34
10.4.1	Context list	34
10.4.2	Abstract syntaxes	34
10.4.3	Presentation user data.....	34
10.4.4	ASN.1 encoding requirements	35
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	36
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	37
11.1.3	Additional presentation protocol requirement	37
11.1.4	Additional ACSE requirements	37
11.2	MMS Authentication value.....	39
11.2.1	General	39
11.2.2	MMS-Authentication value data type	39
11.2.3	Handling of the association request (AARQ-apdu)	40
11.2.4	Handling of the association result (AARE-apdu).....	40
12	End-to-end application security model	41
12.1	Introduction and general architecture	41
12.2	Abstract syntax specifications	42
12.2.1	General	42
13	End-to-end application security (normative)	43
13.1	Association management	43
13.1.1	General concept	43
13.1.2	UTC time specification.....	43
13.1.3	Handshake request.....	43

13.1.4	Handshake accept	44
13.1.5	Association reject by the protected protocol.....	45
13.1.6	Association reject due to security issues.....	45
13.1.7	Handshake security abort	46
13.1.8	Data transfer security abort	46
13.1.9	Abort by protected protocol.....	46
13.1.10	Association release request.....	47
13.1.11	Association release response	47
13.2	Data transfer phase	47
13.2.1	General	47
13.2.2	Clear data transfer.....	48
13.2.3	Encrypted data transfer	48
13.3	ClearToken data types	49
13.3.1	The ClearToken1 data type.....	49
13.3.2	The ClearToken2 data type.....	53
13.3.3	The ClearToken3 data type.....	54
13.4	Authentication and integrity specifications.....	55
13.4.1	The Signature data type	55
13.4.2	The authenticator data type	55
14	E2E security error handling (normative).....	56
14.1	General.....	56
14.2	Specification of diagnostics.....	56
14.2.1	Handshake diagnostics	56
14.2.2	The data transfer diagnostics.....	57
14.3	Checking of E2E-security handshake request and accept	58
14.3.1	General	58
14.3.2	Signature checking	58
14.3.3	Protected protocol identity checking	59
14.3.4	ClearToken1 checking	59
14.4	Checking of security protocol control information during data transfer	60
14.4.1	General	60
14.4.2	Authenticator checking	60
14.4.3	Checks of the ClearToken2 value	60
15	E2E security used in an OSI operational environment.....	61
15.1	General.....	61
15.2	Additional upper layer requirements	61
15.2.1	Additional presentation layer requirements	61
15.2.2	Additional ACSE requirements	61
15.3	Association management in an OSI operational environment	62
15.3.1	General	62
15.3.2	Mapping to ACSE association request	62
15.3.3	Mapping to ACSE association response.....	62
15.3.4	Mapping to ACSE abort	63
15.3.5	Mapping to ACSE release request	64
15.3.6	Mapping to ACSE release response.....	64
15.4	Data transfer in OSI operational environment.....	64
15.4.1	General	64
15.4.2	Mapping of the clear data transfer SecPDU	64
15.4.3	Mapping of the encrypted data transfer SecPDU.....	65

15.5	OSI upper layer routing	65
15.6	OSI operational environment checking	66
15.6.1	General checking.....	66
15.6.2	Environment mapping checking	66
15.6.3	OSI operational environment diagnostics	67
16	E2E security used in in an XMPP operational environment	67
16.1	General on wrapping to an XMPP operational environment.....	67
16.2	Mapping of SecPDUs to iq stanzas	68
16.3	Mapping of SecPDUs to message stanzas	69
16.4	XMPP stanza error handling	69
16.5	XML namespaces	70
16.6	Encoding of EnvPDUs within XMPP stanzas	70
16.7	Multiple associations.....	71
16.8	Release collision consideration	71
17	Conformance to this document	71
17.1	General.....	71
17.2	Notation	71
17.3	Conformance to operational environment	71
17.4	Conformance to modes of operation.....	72
17.5	Conformance to compatibility mode	72
17.6	Conformance to native mode	73
Annex A (normative)	Formal ASN.1 specification for the A-security-profile	75
Annex B (normative)	Formal ASN.1 specification for the End-to-End security.....	76
Annex C (normative)	Formal W3C XSD specification for the end-to-end security	82
Annex D (normative)	ASN.1 module for OSI operational environment	89
D.1	Scope of annex	89
D.2	ASN.1 module.....	89
Annex E (normative)	ASN.1 modules and W3C XSDs for an XMPP operational environment.....	91
E.1	Scope of Annex	91
E.2	ASN.1 modules for the XMPP operational environment	91
E.2.1	ASN.1 module for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	91
E.2.2	ASN.1 module for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	91
E.3	W3C XSDs for the XMPP operational environment.....	93
E.3.1	W3C XSD for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace	93
E.3.2	W3C XSD for the http://www.iec.ch/62351/2018/ENV_4 XML namespace	94
Annex F (normative)	Template for virtual API specifications	96
F.1	General.....	96
F.2	ASN.1 virtual API specification.....	97
F.3	W3C XSD virtual API specification	97
Annex G (normative)	End-entity public-key certificate specification	98
G.1	Scope of annex	98
G.2	General requirement	98
G.3	Length considerations	98
G.4	Basic Structure requirement and recommendations.....	98
G.4.1	Version component.....	98

G.4.2	Serial number component	98
G.4.3	Issuer signature algorithm component	98
G.4.4	Issuer component	99
G.4.5	Validity component	99
G.4.6	Subject component	99
G.4.7	Subject public key Information component	99
G.4.8	Issuer unique ID and subject unique ID components	100
G.5	Extensions	100
G.5.1	General	100
G.5.2	Key usage extension	100
G.5.3	Revocation checking	100
G.5.4	IEC user role information extension	101
G.6	Specific requirements for operational environments	101
G.6.1	General	101
G.6.2	OSI operational environment	101
G.6.3	XMPP operational environment	101
Annex H (normative)	Lower layer requirements for the OSI operational environment	102
H.1	Scope of annex	102
H.2	Transport protocol class 0	102
H.2.1	Enforcement of maximum lengths	102
H.2.2	Response to Class 0 unsupported TPDUs	102
H.2.3	Transport selectors	102
H.3	IETF RFC 1006	103
H.3.1	General	103
H.3.2	Version number	103
H.3.3	Length	103
H.3.4	Keep-alive	103
Annex I (informative)	ASN.1 definition of ACSE	104
Bibliography	108
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 TRANFER SPDU	35	
Figure 5 – E2E security building blocks	41	
Figure 6 – Relationship between environment, E2E-security and protected protocol	41	
Figure 7 – Relationships between APDUs	42	
Figure 8 – The scope of E2E-security specification	42	
Figure 9 – Upper layer routing	65	
Figure F.1 – Virtual API concept	96	
Table 1 – Relationship between security and security measure combinations	19	
Table 2 – Commented recommended cipher suites from IEC TS 62351-4:2007	25	
Table 3 – Cipher suites combinations in the context of this document	26	
Table 4 – Mapping of SecPDUs to ACSE APDUs	62	
Table 5 – Mapping of SecPDUs to XMPP stanzas	68	

Table 6 – Conformance to operational environment	72
Table 7 – Conformance to modes of operation.....	72
Table 8 – Conformance to compatibility mode.....	72
Table 9 – Conformance to TLS cipher suites in compatibility mode	73
Table 10 – Conformance to native mode	73
Table 11 – Conformance to mode of encryption	73
Table 12 – Conformance to TLS cipher suites in native mode	74
Table 13 – Conformance to cryptographic algorithms for E2E-security	74
Table H.1 – TP class 0 maximum sizes	102

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.

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

This bilingual version (2020-01) corresponds to the monolingual English version, published in 2018-11.

The text of this standard is based on the following documents:

FDIS	Report on voting
57/2032/FDIS	57/2053/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

The French version of this standard has not been voted upon.

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 this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

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

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

Part 4: Profiles including MMS and derivatives

1 Scope

1.1 General

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

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

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

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

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

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

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

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

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

¹ Numbers in square brackets refer to the bibliography.

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

1.2 Code components

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

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

IEC 62351-3:2014/AMD1:2018

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

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

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

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

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

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

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

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

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

ISO/IEC 9594-8: | Rec. ITU-T X.509, *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	116
1 Domaine d'application	118
1.1 Généralités	118
1.2 Composantes de code	119
2 Références normatives	119
3 Termes, définitions et termes abrégés	121
3.1 Généralités	121
3.2 Termes et définitions	121
3.3 Termes abrégés	125
4 Problèmes de sécurité couverts par la présente partie de l'IEC 62351	126
4.1 Modèles de référence pour la communication	126
4.2 Sécurité des profils application et transport	126
4.3 Mode compatible et mode natif	127
4.4 Menaces à la sécurité contrées	127
4.4.1 Généralités	127
4.4.2 Menaces contrées en mode compatible	128
4.4.3 Menaces contrées en mode natif	128
4.5 Méthodes d'attaque contrées	128
4.5.1 Généralités	128
4.5.2 Attaques contrées en mode compatible	128
4.5.3 Attaques contrées en mode natif	129
4.6 Journalisation	129
5 Exigences spécifiques	130
5.1 Exigences spécifiques concernant la pile communication ICCP/IEC 60870-6-x	130
5.2 Exigences spécifiques concernant l'IEC 61850	130
6 Sécurité de transport	131
6.1 Généralités	131
6.2 Application de la sécurité de couche de transport (TLS)	131
6.2.1 Généralités	131
6.2.2 Concept de suite chiffrée TLS	131
6.2.3 Reprise de session TLS	131
6.2.4 Renégociation de session TLS	131
6.2.5 Nombre d'ancrages sécurisés pris en charge	132
6.2.6 Taille de certificat de clé publique	132
6.2.7 Période d'évaluation relative à l'état de révocation des certificats de clé publique	132
6.2.8 Validation de certificat de clé publique	132
6.2.9 Traitement des événements de sécurité	132
6.3 Sécurité de type T dans un environnement d'exploitation OSI	133
6.3.1 Généralités	133
6.3.2 Accès TCP	133
6.3.3 Désactivation de la TLS	133
6.3.4 Prise en charge des suites chiffrées TLS	133
6.4 Sécurité de type T dans un environnement d'exploitation XMPP	135
7 Vue d'ensemble concernant la sécurité de la couche application (informative)	135
7.1 Généralités	135

7.2	Techniques de description	136
7.2.1	Généralités	136
7.2.2	ASN.1 en tant que définition de schéma XML	136
7.2.3	Définition de schéma W3C XML (W3C XSD).....	137
7.2.4	Espace de nommage XML	137
8	Utilisation d'algorithmes cryptographiques	137
8.1	Généralités	137
8.2	Définitions cryptographiques de base.....	137
8.3	Algorithmes de clé publique	138
8.4	Algorithmes de hachage.....	139
8.5	Algorithmes de signature	139
8.6	Algorithmes de chiffrement symétrique utilisés uniquement pour le chiffrement.....	139
8.7	Algorithmes de chiffrement authentifié	140
8.8	Algorithmes de valeur de vérification d'intégrité	140
9	Attribution d'identifiant d'objet (normatif)	141
10	Exigences générales relatives à la couche supérieure OSI (normatif)	141
10.1	Vue d'ensemble	141
10.2	Généralités concernant les exigences relatives à la couche supérieure OSI.....	142
10.3	Exigences relatives au protocole de session	142
10.4	Exigences relatives au protocole de présentation.....	143
10.4.1	Liste contextuelle.....	143
10.4.2	Syntaxes abstraites	143
10.4.3	Données d'utilisateur de présentation	144
10.4.4	Exigences relatives au codage ASN.1.....	145
10.5	Exigences relatives au protocole d'élément de service de contrôle d'association (ACSE)	145
10.5.1	Généralités.....	145
10.5.2	Version de protocole.....	145
10.5.3	Titres	145
10.5.4	Utilisation du type de donnée ASN.1 EXTERNAL.....	146
11	Profil de sécurité de type A (normatif).....	146
11.1	Exigences OSI spécifiques au profil de sécurité de type A	146
11.1.1	Généralités.....	146
11.1.2	Exigences supplémentaires relatives au protocole de session	146
11.1.3	Exigence supplémentaire relative au protocole de présentation	147
11.1.4	Exigences supplémentaires relatives à ACSE	147
11.2	Valeur d'authentification MMS.....	148
11.2.1	Généralités.....	148
11.2.2	Type de données de valeur d'authentification MMS	148
11.2.3	Traitement des demandes d'association (AARQ-apdu)	149
11.2.4	Traitement du résultat d'association (AARE-apdu)	149
12	Modèle de sécurité d'application bout-à-bout.....	150
12.1	Introduction et architecture générale	150
12.2	Spécifications relatives à la syntaxe abstraite	152
12.2.1	Généralités	152
13	Sécurité d'application bout-à-bout (normatif)	152
13.1	Gestion d'association	152
13.1.1	Concept général	152

13.1.2	Spécification relative au temps UTC	153
13.1.3	Demande d'établissement de liaison	153
13.1.4	Acceptation d'établissement de liaison	154
13.1.5	Rejet d'association par le protocole protégé	154
13.1.6	Rejet d'association dû à des questions de sécurité	155
13.1.7	Abandon d'établissement de liaison pour raison de sécurité	155
13.1.8	Abandon de transfert de données pour raison de sécurité	155
13.1.9	Abandon par protocole protégé	156
13.1.10	Demande de libération d'association	156
13.1.11	Réponse de libération d'association	157
13.2	Phase de transfert de données	157
13.2.1	Généralités	157
13.2.2	Transfert de données en clair	157
13.2.3	Transfert de données chiffrées	157
13.3	Types de données ClearToken	158
13.3.1	Le type de données ClearToken1	158
13.3.2	Le type de données ClearToken2	164
13.3.3	Le type de données ClearToken3	165
13.4	Spécifications d'authentification et d'intégrité	165
13.4.1	Le type de données Signature	165
13.4.2	Le type de données Authenticateur	166
14	Traitement des erreurs de sécurité E2E (normatif)	166
14.1	Généralités	166
14.2	Spécification des diagnostics	166
14.2.1	Diagnostics d'établissement de liaison	166
14.2.2	Diagnostics de transfert de données	168
14.3	Vérification de la demande et de l'acceptation de l'établissement de liaison pour la sécurité E2E	169
14.3.1	Généralités	169
14.3.2	Vérification de signature	169
14.3.3	Vérification d'identité de protocole protégé	169
14.3.4	Vérification de ClearToken1	169
14.4	Vérification des informations de contrôle du protocole de sécurité lors du transfert de données	170
14.4.1	Généralités	170
14.4.2	Vérification de l'authenticateur	171
14.4.3	Vérifications de la valeur de ClearToken2	171
15	Sécurité E2E utilisée dans un environnement d'exploitation OSI	171
15.1	Généralités	171
15.2	Exigences supplémentaires relatives à la couche supérieure	171
15.2.1	Exigences supplémentaires relatives à la couche de présentation	171
15.2.2	Exigences supplémentaires relatives à l'ACSE	172
15.3	Gestion d'association dans un environnement d'exploitation OSI	172
15.3.1	Généralités	172
15.3.2	Mise en correspondance avec la demande d'association ACSE	173
15.3.3	Mise en correspondance avec la réponse d'association ACSE	173
15.3.4	Mise en correspondance avec l'abandon ACSE	174
15.3.5	Mise en correspondance avec la demande de libération ACSE	174
15.3.6	Mise en correspondance avec la réponse de libération ACSE	175

15.4	Transfert de données dans un environnement d'exploitation OSI	175
15.4.1	Généralités	175
15.4.2	Mise en correspondance de la SecPDU de transfert de données en clair	175
15.4.3	Mise en correspondance de la SecPDU de transfert de données chiffrées	175
15.5	Acheminement de la couche supérieure OSI	175
15.6	Vérifications relatives à un environnement d'exploitation OSI.....	177
15.6.1	Vérifications générales	177
15.6.2	Vérification de la mise en correspondance d'environnement	177
15.6.3	Diagnostics relatifs à un environnement d'exploitation OSI	178
16	Sécurité E2E utilisée dans un environnement d'exploitation XMPP	178
16.1	Généralités sur l'enveloppement à un environnement d'exploitation XMPP	178
16.2	Mise en correspondance des SecPDU avec les strophes iq	179
16.3	Mise en correspondance des SecPDU avec les strophes message	180
16.4	Traitement des erreurs de strophe XMPP.....	180
16.5	Espaces de nommage XML.....	181
16.6	Codage des EnvPDU dans les strophes XMPP	181
16.7	Associations multiples.....	181
16.8	Prise en considération des collisions de libération	181
17	Conformité au présent document	182
17.1	Généralités	182
17.2	Notation	182
17.3	Conformité à l'environnement d'exploitation	182
17.4	Conformité aux modes d'exploitation.....	183
17.5	Conformité au mode compatible.....	183
17.6	Conformité au mode natif.....	184
Annex A (normative)	Spécification ASN.1 officielle concernant le profil de sécurité de type A	186
Annex B (normative)	Spécification ASN.1 officielle concernant la sécurité E2E	187
Annex C (normative)	Spécification W3C XSD officielle concernant la sécurité E2E	193
Annex D (normative)	Module ASN.1 pour un environnement d'exploitation OSI.....	200
D.1	Domaine d'application de l'Annexe	200
D.2	Module ASN.1.....	200
Annex E (normative)	Modules ASN.1 et W3C XSD pour un environnement d'exploitation XMPP	202
E.1	Domaine d'application de l'Annexe	202
E.2	Modules ASN.1 pour l'environnement d'exploitation XMPP	202
E.2.1	Module ASN.1 pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas	202
E.2.2	Module ASN.1 pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	202
E.3	Modules W3C XSD pour l'environnement d'exploitation XMPP	204
E.3.1	W3C XSD pour l'espace de nommage XML urn:ietf:params:xml:ns:xmpp-stanzas	204
E.3.2	W3C XSD pour l'espace de nommage XML http://www.iec.ch/62351/2018/ENV_4	205
Annex F (normative)	Modèle pour spécifications relatives aux API virtuelles	207
F.1	Généralités	207
F.2	Spécification relative à l'API virtuelle ASN.1	208

F.3	Spécification relative à l'API virtuelle W3C XSD	208
Annex G (normative)	Spécification relative au certificat de clé publique d'entité finale	209
G.1	Domaine d'application de l'Annexe	209
G.2	Exigences générales	209
G.3	Considérations concernant la longueur	209
G.4	Exigences et recommandations relatives à la structure de base	209
G.4.1	Composante version	209
G.4.2	Composante numéro de série	209
G.4.3	Composante algorithme de signature de l'émetteur	210
G.4.4	Composante émetteur	210
G.4.5	Composante validité	210
G.4.6	Composante sujet	210
G.4.7	Composante information de clé publique sujet	210
G.4.8	Composantes Identifiant unique d'émetteur et Identifiant unique de sujet	211
G.5	Extensions	211
G.5.1	Généralités	211
G.5.2	Extension utilisation de clé	211
G.5.3	Vérification de révocation	211
G.5.4	Extension information concernant le rôle de l'utilisateur de l'IEC	212
G.6	Exigences spécifiques relatives aux environnements d'exploitation	212
G.6.1	Généralités	212
G.6.2	Environnement d'exploitation OSI	212
G.6.3	Environnement d'exploitation XMPP	212
Annex H (normative)	Exigences relatives à la couche inférieure dans un environnement d'exploitation OSI	213
H.1	Domaine d'application de l'Annexe	213
H.2	Protocole de transport de classe 0	213
H.2.1	Application des longueurs maximales	213
H.2.2	Réponse aux TPDU non pris en charge par la classe 0	213
H.2.3	Sélecteurs de transport	213
H.3	RFC 1006 de l'IETF	214
H.3.1	Généralités	214
H.3.2	Numéro de version	214
H.3.3	Longueur	214
H.3.4	Keepalive	214
Annex I (informative)	Définition ASN.1 de l'ACSE	215
Bibliographie	219	
Figure 1 – Profils application et transport (informatif)	126	
Figure 2 – Profils de type T sans et avec protection TLS	133	
Figure 3 – Établissement d'association	142	
Figure 4 – Inclusion des données utilisateur dans la SPDU SESSION DATA TRANSFER	144	
Figure 5 – Blocs de construction de sécurité E2E	150	
Figure 6 – Relation entre environnement, sécurité E2E et protocole protégé	151	
Figure 7 – Relations entre APDU	151	
Figure 8 – Domaine d'application de la spécification concernant la sécurité E2E	151	

Figure 9 – Acheminement de la couche supérieure	176
Figure F.1 – Concept d'API virtuelle.....	207
Tableau 1 – Relation entre la sécurité et les combinaisons de mesures de sécurité	127
Tableau 2 - Suites chiffrées recommandées et commentées de l'IEC TS 62351-4:2007	134
Tableau 3 - Combinaisons de suites chiffrées dans le contexte du présent document	135
Tableau 4 – Mise en correspondance des SecPDU avec les APDU de l'ACSE	172
Tableau 5 – Mise en correspondance des SecPDU avec les strophes XMPP	178
Tableau 6 – Conformité à l'environnement d'exploitation	182
Tableau 7 – Conformité aux modes d'exploitation	183
Tableau 8 – Conformité au mode compatible	183
Tableau 9 – Conformité aux suites chiffrées TLS en mode compatible	183
Tableau 10 – Conformité au mode natif.....	184
Tableau 11 – Conformité aux modes de chiffrement.....	184
Tableau 12 – Conformité aux suites chiffrées TLS en mode natif	184
Tableau 13 – Conformité aux algorithmes cryptographiques pour la sécurité E2E	185
Tableau H.1 – Tailles maximales de protocole de transport de classe 0	213

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.

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.

La présente version bilingue (2020-01) correspond à la version anglaise monolingue publiée en 2018-11.

Le texte anglais de cette norme est issu des documents 57/2032/FDIS et 57/2053/RVD.

Le rapport de vote 57/2053/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

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 **bold 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 **bold 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 ce document 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. À 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 ce document 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: | Rec. UIT-T X.509, *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*