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.

IEC 62351-4

Edition 1.1 2020-07

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

IEC 62351-4:2018-1+AMD1:2020-07 CSV(en-fr)

CONTENTS

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 **`bold 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 **`bold Courier New`** typeface.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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- withdrawn,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

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

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

Part 4: Profiles including MMS and derivatives

1 Scope

1.1 General

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

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

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

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

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

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

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

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

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

---

[1] Numbers in square brackets refer to the bibliography.

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

1.2 Code components

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

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

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

2 Normative references

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

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

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

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD1:2018

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SOMMAIRE

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 **`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 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*

IEC 62351-4

Edition 1.1 2020-07

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

IEC 62351-4:2018-1+AMD1:2020-07 CSV(en-fr)

CONTENTS

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 **`bold 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 **`bold Courier New`** typeface.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

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

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

Part 4: Profiles including MMS and derivatives

1 Scope

1.1 General

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

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

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

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

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

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

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

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

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

---

[1] Numbers in square brackets refer to the bibliography.

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

1.2 Code components

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

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

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

2 Normative references

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

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

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

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD1:2018

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SOMMAIRE

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 **`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 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*