IEC 62351-3

Edition 1.2 2020-02
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-7772-0

IEC 62351-3

Edition 1.2 2020-02
CONSOLIDATED VERSION

REDLINE VERSION

VERSION REDLINE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

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 62351-3:2014-10+AMD1:2018-05+AMD2:2020-02 CSV(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 3: Communication network and system security – Profiles including TCP/IP

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 amendments has been prepared for user convenience.

IEC 62351-3 edition 1.2 contains the first edition (2014-10) [documents 57/1498/FDIS and 57/1515/RVD], its amendment 1 (2018-05) [documents 57/1976/FDIS and 57/1990/RVD] and its amendment 2 (2020-02) [documents 57/2149/FDIS and 57/2167/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendments 1 and 2. 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 62351-3 has been prepared by IEC technical committee 57: Power systems management and associated information 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.

The committee has decided that the contents of the base publication and its amendments 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.

INTRODUCTION to Amendment 2

This amendment to International Standard IEC 62351-3 has been prepared in order to address the following issues:

– Support for TLS versions 1.1 and 1.0 is made optional instead of mandatory to address known weaknesses. This is aligned with the defined security warnings for TLS versions 1.1 and 1.0.

– Update of TLS version handling during renegotiation and resumption to avoid TLS version downgrade/upgrade within a same session.

– Updated explanatory text for session renegotiation to make the communication relations clearer.

– Deprecation of RSA1024 and SHA-1 algorithms. This underlines the desire to disallow them in the next edition.

– Inclusion of PICS section for mandatory and optional settings in TLS.

– Updated text for and enhancements of security events to better align with IEC 62351-14

– Inclusion of general remarks for the security event handling.

– Update of references.

Moreover, explanatory text has been included to better describe certain options as well as an adjustment to the requirements for referencing standards.

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

Part 3: Communication network and system security – Profiles including TCP/IP

1 Scope

1.1 Scope

This part of IEC 62351 specifies how to provide confidentiality, integrity protection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer when cyber-security is required.

Although there are many possible solutions to secure TCP/IP, the particular scope of this part is to provide security between communicating entities at either end of a TCP/IP connection within the end communicating entities. The use and specification of intervening external security devices (e.g. “bump-in-the-wire”) are considered out-of-scope.

This part of IEC 62351 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 5246) so that they are applicable to the telecontrol environment of the IEC. TLS is applied to protect the TCP communication. It is intended that this standard be referenced as a normative part of other IEC standards that have the need for providing security for their TCP/IP-based protocol. However, it is up to the individual protocol security initiatives to decide if this standard is to be referenced.

This part of IEC 62351 reflects the security requirements of the IEC power systems management protocols. Should other standards bring forward new requirements, this standard may need to be revised.

1.2 Intended Audience

The initial audience for this specification is intended to be experts developing or making use of IEC protocols in the field of power systems management and associated information exchange. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves, where the protocols make use of TCP/IP security. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC ~~TS~~ 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment* [1]

ISO/IEC 9594-8:2017, *Rec. ITU-T X.509 (2016), Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

RFC 4492:2006, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*

RFC 5246:2008, *The TLS Protocol Version 1.2*[2]

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension*

RFC 6066:2006, *Transport Layer Security Extensions*

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*

---

[1] ~~Under consideration.~~

[2] This is typically referred to as SSL/TLS.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique 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. A 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 ses amendements a été préparée pour la commodité de l'utilisateur.

L'IEC 62351-3 édition 1.2 contient la première édition (2014-10) [documents 57/1498/FDIS et 57/1515/RVD], son amendement 1 (2018-05) [documents 57/1976/FDIS et 57/1990/RVD] et son amendement 2 (2020-02) [documents 57/2149/FDIS et 57/2167/RVD].

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par les amendements 1 et 2. 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 Norme internationale IEC 62351-3 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Cette publication a été rédigée 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.

Le comité a décidé que le contenu de la publication de base et de ses amendements 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.

INTRODUCTION à l'Amendement 2

Le présent amendement à la Norme internationale IEC 62351-3 a été établi afin de traiter les points suivants:

– Prise en charge des versions TLS 1.1 et 1.0 rendue facultative plutôt qu'obligatoire pour remédier aux faiblesses connues. Cette possibilité permet de s'aligner sur les avertissements de sécurité définis pour les versions TLS 1.1 et 1.0.

– Mise à jour de la gestion des versions TLS lors de la renégociation et de la reprise pour éviter une mise à niveau inférieur/supérieur des versions TLS au cours d'une même session.

– Mise à jour du texte explicatif de la renégociation de session pour clarifier davantage les relations de communication.

– Rejet des algorithmes RSA1024 et SHA-1. Cette démarche souligne la volonté de les interdire dans la prochaine édition.

– Inclusion de la section des PICS pour les paramètres obligatoires et facultatifs dans la TLS.

– Mise à jour du texte et améliorations des événements de sécurité pour mieux s'aligner sur l'IEC 62351-14.

– Inclusion de remarques générales sur la gestion des événements de sécurité.

– Mise à jour des références.

De plus, un texte explicatif permettant de mieux décrire certaines options a été inclus ainsi qu'un ajustement des exigences relatives aux normes de référence.

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

1 Domaine d'application

1.1 Domaine d'application

La présente partie de l'IEC 62351 spécifie comment garantir la confidentialité, la protection de l'intégrité et l'authentification des niveaux des messages pour les protocoles SCADA (système de commande, de surveillance et d'acquisition de données, *Supervisory Control And Data Acquisition*) et de téléconduite qui utilisent les protocoles TCP/IP comme couche transport des messages lorsque la cybersécurité est exigée.

Bien qu'il existe de nombreuses solutions permettant de sécuriser les protocoles TCP/IP, le domaine d'application de la présente partie est de sécuriser la communication entre des entités, à l'une ou l'autre extrémité de la connexion TCP/IP, dans les limites des entités communicantes. L'utilisation et la spécification des dispositifs de sécurité externe concernés (par exemple, "bump-in-the-wire") sont considérées comme ne relevant pas du domaine d'application de la présente norme.

La présente partie de l'IEC 62351 spécifie comment garantir la sécurité des protocoles basés sur les TCP/IP par des contraintes relatives à la spécification des messages, des procédures et des algorithmes de TLS (sécurité de la couche transport, *Transport Layer Security*) (définis dans la RFC 5246), afin qu'ils s'appliquent à l'environnement de téléconduite de l'IEC. La TLS est appliquée afin de protéger la communication TCP. Il est prévu que la présente norme soit référencée comme partie normative des autres normes IEC qui traitent de la nécessité de garantir la sécurité de leurs protocoles basés sur les TCP/IP. Cependant, il revient aux initiatives individuelles concernant la sécurité des protocoles de décider si la présente norme doit être référencée.

La présente partie de l'IEC 62351 présente les exigences de sécurité des protocoles de la gestion des systèmes de puissance de l'IEC. Si d'autres normes ajoutent des exigences supplémentaires, il peut être nécessaire de réviser la présente norme.

1.2 Utilisateurs prévus

Les premiers utilisateurs auxquels s'adresse la présente spécification sont les experts qui conçoivent ou utilisent les protocoles IEC dans le domaine de la gestion des systèmes de puissance et échanges d'informations associés. Pour que les mesures décrites dans la présente spécification soient mises en œuvre, elles doivent être acceptées et référencées dans les spécifications pour les protocoles eux-mêmes lorsqu'ils utilisent la sécurité TCP/IP. Le présent document est rédigé afin de permettre ce processus.

Les autres utilisateurs auxquels s'adresse la présente spécification sont les concepteurs de produits appliquant ces protocoles.

Des parties de la présente spécification peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 les éventuels amendements).

IEC TS 62351-1:2007, *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 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models (disponible en anglais seulement)*

IEC ~~TS~~ 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment* [1] (disponible en anglais seulement)

ISO/IEC 9594-8:2017, *Rec. ITU-T X.509 (2016), Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: – Partie 8: Cadre général des certificats de clé publique et d'attribut*

RFC 4492:2006, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)* (disponible en anglais seulement)

RFC 5246:2008, *The TLS Protocol Version 1.2*[2] (disponible en anglais seulement)

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (disponible en anglais seulement)

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension* (disponible en anglais seulement)

RFC 6066:2006, *Transport Layer Security Extensions* (disponible en anglais seulement)

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0* (disponible en anglais seulement)

---

[1] ~~A l'étude.~~

[2] Généralement appelé SSL/TLS.

IEC 62351-3

Edition 1.2 2020-02
CONSOLIDATED VERSION

FINAL VERSION

VERSION FINALE

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 3: Communication network and system security – Profiles including TCP/IP

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 62351-3:2014-10+AMD1:2018-05+AMD2:2020-02 CSV(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 3: Communication network and system security – Profiles including TCP/IP

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 amendments has been prepared for user convenience.

IEC 62351-3 edition 1.2 contains the first edition (2014-10) [documents 57/1498/FDIS and 57/1515/RVD], its amendment 1 (2018-05) [documents 57/1976/FDIS and 57/1990/RVD] and its amendment 2 (2020-02) [documents 57/2149/FDIS and 57/2167/RVD].

This Final version does not show where the technical content is modified by amendments 1 and 2. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 62351-3 has been prepared by IEC technical committee 57: Power systems management and associated information 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.

The committee has decided that the contents of the base publication and its amendments 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.

INTRODUCTION to Amendment 2

This amendment to International Standard IEC 62351-3 has been prepared in order to address the following issues:

– Support for TLS versions 1.1 and 1.0 is made optional instead of mandatory to address known weaknesses. This is aligned with the defined security warnings for TLS versions 1.1 and 1.0.

– Update of TLS version handling during renegotiation and resumption to avoid TLS version downgrade/upgrade within a same session.

– Updated explanatory text for session renegotiation to make the communication relations clearer.

– Deprecation of RSA1024 and SHA-1 algorithms. This underlines the desire to disallow them in the next edition.

– Inclusion of PICS section for mandatory and optional settings in TLS.

– Updated text for and enhancements of security events to better align with IEC 62351-14

– Inclusion of general remarks for the security event handling.

– Update of references.

Moreover, explanatory text has been included to better describe certain options as well as an adjustment to the requirements for referencing standards.

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

Part 3: Communication network and system security – Profiles including TCP/IP

1 Scope

1.1 Scope

This part of IEC 62351 specifies how to provide confidentiality, integrity protection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer when cyber-security is required.

Although there are many possible solutions to secure TCP/IP, the particular scope of this part is to provide security between communicating entities at either end of a TCP/IP connection within the end communicating entities. The use and specification of intervening external security devices (e.g. “bump-in-the-wire”) are considered out-of-scope.

This part of IEC 62351 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 5246) so that they are applicable to the telecontrol environment of the IEC. TLS is applied to protect the TCP communication. It is intended that this standard be referenced as a normative part of other IEC standards that have the need for providing security for their TCP/IP-based protocol. However, it is up to the individual protocol security initiatives to decide if this standard is to be referenced.

This part of IEC 62351 reflects the security requirements of the IEC power systems management protocols. Should other standards bring forward new requirements, this standard may need to be revised.

1.2 Intended Audience

The initial audience for this specification is intended to be experts developing or making use of IEC protocols in the field of power systems management and associated information exchange. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves, where the protocols make use of TCP/IP security. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

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

ISO/IEC 9594-8:2017, *Rec. ITU-T X.509 (2016), Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

RFC 4492:2006, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*

RFC 5246:2008, *The TLS Protocol Version 1.2*[1]

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension*

RFC 6066:2006, *Transport Layer Security Extensions*

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*

---

1 This is typically referred to as SSL/TLS.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique 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. A 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 ses amendements a été préparée pour la commodité de l'utilisateur.

L'IEC 62351-3 édition 1.2 contient la première édition (2014-10) [documents 57/1498/FDIS et 57/1515/RVD], son amendement 1 (2018-05) [documents 57/1976/FDIS et 57/1990/RVD] et son amendement 2 (2020-02) [documents 57/2149/FDIS et 57/2167/RVD].

Cette version Finale ne montre pas les modifications apportées au contenu technique par les amendements 1 et 2. Une version Redline montrant toutes les modifications est disponible dans cette publication.

La Norme internationale IEC 62351-3 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Cette publication a été rédigée 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.

Le comité a décidé que le contenu de la publication de base et de ses amendements 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.

INTRODUCTION à l'Amendement 2

Le présent amendement à la Norme internationale IEC 62351-3 a été établi afin de traiter les points suivants:

– Prise en charge des versions TLS 1.1 et 1.0 rendue facultative plutôt qu'obligatoire pour remédier aux faiblesses connues. Cette possibilité permet de s'aligner sur les avertissements de sécurité définis pour les versions TLS 1.1 et 1.0.

– Mise à jour de la gestion des versions TLS lors de la renégociation et de la reprise pour éviter une mise à niveau inférieur/supérieur des versions TLS au cours d'une même session.

– Mise à jour du texte explicatif de la renégociation de session pour clarifier davantage les relations de communication.

– Rejet des algorithmes RSA1024 et SHA-1. Cette démarche souligne la volonté de les interdire dans la prochaine édition.

– Inclusion de la section des PICS pour les paramètres obligatoires et facultatifs dans la TLS.

– Mise à jour du texte et améliorations des événements de sécurité pour mieux s'aligner sur l'IEC 62351-14.

– Inclusion de remarques générales sur la gestion des événements de sécurité.

– Mise à jour des références.

De plus, un texte explicatif permettant de mieux décrire certaines options a été inclus ainsi qu'un ajustement des exigences relatives aux normes de référence.

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

1 Domaine d'application

1.1 Domaine d'application

La présente partie de l'IEC 62351 spécifie comment garantir la confidentialité, la protection de l'intégrité et l'authentification des niveaux des messages pour les protocoles SCADA (système de commande, de surveillance et d'acquisition de données, *Supervisory Control And Data Acquisition*) et de téléconduite qui utilisent les protocoles TCP/IP comme couche transport des messages lorsque la cybersécurité est exigée.

Bien qu'il existe de nombreuses solutions permettant de sécuriser les protocoles TCP/IP, le domaine d'application de la présente partie est de sécuriser la communication entre des entités, à l'une ou l'autre extrémité de la connexion TCP/IP, dans les limites des entités communicantes. L'utilisation et la spécification des dispositifs de sécurité externe concernés (par exemple, "bump-in-the-wire") sont considérées comme ne relevant pas du domaine d'application de la présente norme.

La présente partie de l'IEC 62351 spécifie comment garantir la sécurité des protocoles basés sur les TCP/IP par des contraintes relatives à la spécification des messages, des procédures et des algorithmes de TLS (sécurité de la couche transport, *Transport Layer Security*) (définis dans la RFC 5246), afin qu'ils s'appliquent à l'environnement de téléconduite de l'IEC. La TLS est appliquée afin de protéger la communication TCP. Il est prévu que la présente norme soit référencée comme partie normative des autres normes IEC qui traitent de la nécessité de garantir la sécurité de leurs protocoles basés sur les TCP/IP. Cependant, il revient aux initiatives individuelles concernant la sécurité des protocoles de décider si la présente norme doit être référencée.

La présente partie de l'IEC 62351 présente les exigences de sécurité des protocoles de la gestion des systèmes de puissance de l'IEC. Si d'autres normes ajoutent des exigences supplémentaires, il peut être nécessaire de réviser la présente norme.

1.2 Utilisateurs prévus

Les premiers utilisateurs auxquels s'adresse la présente spécification sont les experts qui conçoivent ou utilisent les protocoles IEC dans le domaine de la gestion des systèmes de puissance et échanges d'informations associés. Pour que les mesures décrites dans la présente spécification soient mises en œuvre, elles doivent être acceptées et référencées dans les spécifications pour les protocoles eux-mêmes lorsqu'ils utilisent la sécurité TCP/IP. Le présent document est rédigé afin de permettre ce processus.

Les autres utilisateurs auxquels s'adresse la présente spécification sont les concepteurs de produits appliquant ces protocoles.

Des parties de la présente spécification peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 les éventuels amendements).

IEC TS 62351-1:2007, *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 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models (disponible en anglais seulement)*

IEC 62351-9, *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 9594-8:2017, *Rec. ITU-T X.509 (2016), Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: – Partie 8: Cadre général des certificats de clé publique et d'attribut*

RFC 4492:2006, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)* (disponible en anglais seulement)

RFC 5246:2008, *The TLS Protocol Version 1.2*[1] (disponible en anglais seulement)

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (disponible en anglais seulement)

RFC 5746:2010, *Transport Layer Security (TLS) Renegotiation Indication Extension* (disponible en anglais seulement)

RFC 6066:2006, *Transport Layer Security Extensions* (disponible en anglais seulement)

RFC 6176:2011, *Prohibiting Secure Sockets Layer (SSL) Version 2.0* (disponible en anglais seulement)

---

1 Généralement appelé SSL/TLS.