IEC 62351-3

Edition 2.0 2023-06

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 978-2-8322-6935-0

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
1.1 Scope 8
1.2 Intended audience 8
2 Normative references 9
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 10
4 Security issues addressed by this document 10
4.1 General 10
4.2 Security threats countered 11
4.3 Attack methods countered 11
4.4 Handling of security events 12
5 Overview of differences in TLS versions 12
5.1 General 12
5.2 Main differences between TLSv1.2 and TLSv1.3 12
5.3 Cipher suite naming 13
5.4 Backward compatibility 14
5.5 Extensions 14
6 Generic requirements 15
6.1 General 15
6.2 Signalling of supported TLS versions 15
6.3 Usage of non-encrypting cipher suites 16
6.4 Certificate support 17
6.4.1 Support of multiple trust anchors 17
6.4.2 Certificate size 17
6.4.3 Certificate exchange 17
6.4.4 Public-key certificate validation 18
6.5 Co-existence with non-secure protocol traffic 21
7 Requirements specific to TLSv1.2 21
7.1 General 21
7.2 Supported cipher suites 21
7.3 Disallowed cipher suites 22
7.4 Key exchange 22
7.4.1 General 22
7.4.2 Key exchange mechanisms 22
7.4.3 Cryptographic algorithms 22
7.4.4 Session resumption 24
7.4.5 Session renegotiation 25
7.5 Support of extensions 26
7.5.1 General 26
7.5.2 TLS session renegotiation extension 26
7.5.3 Signalling of client supported CA certificates via Trusted CA 27
7.5.4 Signalling of supported signature algorithms 27
7.5.5 Stapling of OCSP response messages 28

7.5.6 Signalling of intended target TLS server via Server Name Indication 29
7.5.7 Support of encryption before authentication 29
8 Requirements specific to TLSv1.3 30
8.1 General 30
8.2 Supported cipher suites 30
8.3 Key exchange 30
8.3.1 General 30
8.3.2 Handshake modes 31
8.3.3 Diffie-Hellman Groups 32
8.3.4 Signature algorithms 32
8.4 Session key update (post-handshake message) 33
8.5 New session ticket (post-handshake message) 34
8.6 Session resumption 34
8.7 Certificate validation 34
8.8 Support of extensions 35
8.8.1 General 35
8.8.2 Signalling of supported TLS versions 35
8.8.3 Cookie 35
8.8.4 Signalling of supported signature algorithms 35
8.8.5 Signalling of supported groups 36
8.8.6 Signalling of key share 36
8.8.7 Signalling of intended target TLS server via Server Name Indication 36
8.8.8 Signalling of supported certificate authorities 37
8.8.9 Support of PSK based key agreement 37
8.8.10 Stapling of OCSP response messages 37
8.8.11 Signalling of early data 38
9 Optional security measure support 38
10 Conformance 38
10.1 General 38
10.2 Notation 38
10.3 Conformance to selected TLS versions 38
10.4 Conformance to certificate handling 39
10.5 Conformance to TLSv1.2 specifics 39
10.5.1 Conformance to selected cipher suites 39
10.5.2 Conformance to cryptographic algorithm support 40
10.5.3 Conformance to TLSv1.2 session management features 40
10.5.4 Conformance to selected TLSv1.2 extensions 41
10.6 Conformance to TLSv1.3 specifics 41
10.6.1 Conformance to selected TLSv1.3 cipher suites 41
10.6.2 Conformance to selected TLSv1.3 session management features 42
10.6.3 Conformance to selected TLSv1.3 extensions 44
10.6.4 Conformance to selected TLSv1.3 post-handshake messages 44
Annex A (informative) Security Events 46
A.1 Security event logs 46
A.2 Mapping of TLS events related to the TLS handshake 46
A.3 Mapping of TLS events related to the certificate handling 48
Bibliography 49

Figure 1 – Definition of cipher suites according to TLSv1.2 (RFC 5246) 14
Figure 2 – Definition of cipher suites according to TLSv1.3 (RFC 8446) 14

Table 1 – Support of cipher suites for TLSv1.2 21
Table 2 – Support of cipher suites for TLSv1.3 30
Table 3 – Support of PSK-based handshake modes for TLSv1.3 31
Table 4 – Support of Diffie Hellman Groups for TLSv1.3 32
Table 5 – Supported signature algorithms for the handshake in TLSv1.3 32
Table 6 – Supported signature algorithms for the certificates in TLSv1.3 33
Table 7 – Conformance to TLS versions 38
Table 8 – Conformance to certificate support 39
Table 9 – Conformance to TLSv1.2 usable cipher suites 40
Table 10 – Conformance to cryptographic algorithm support 40
Table 11 – Conformance to TLSv1.2 session management features 41
Table 12 – Conformance to TLSv1.2 handshake extensions 41
Table 13 – Conformance to TLSv1.3 cipher suites 42
Table 14 – Conformance to handshake modes of TLSv1.3 42
Table 15 –Conformance to early data feature (0-RTT) of TLSv1.3 42
Table 16 – Conformance to supported Diffie Hellman Groups in TLSv1.3 43
Table 17 – Conformance to supported signature algorithms for the handshake in TLSv1.3 43
Table 18 – Conformance to supported signature algorithms for the certificates in TLSv1.3 44
Table 19 – Conformance to TLSv1.3 extensions 44
Table 20 – Conformance to post-handshake messages of TLSv1.3 45
Table A.1 – Security event logs related to TLS handshake defined in IEC 62351-3:— (Ed.2) mapped to IEC 62351-14 46
Table A.2 – Security event logs related to certificate validation defined in IEC 62351-3 Ed.2 mapped to IEC 62351-14 48

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.

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

This second edition cancels and replaces the first edition published in 2014, Amendment 1:2018 and Amendment 2:2020. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Inclusion of the TLSv1.2 related parameter required in IEC 62351-3 Ed.1.2 to be specified by the referencing standard. This comprises the following parameter:
   - Mandatory TLSv1.2 cipher suites to be supported.
   - Specification of session resumption parameters.
   - Specification of session renegotiation parameters.

- Revocation handling using CRL and OCSP.
- Handling of security events.

b) Inclusion of a TLSv1.3 profile to be applicable for the power system domain in a similar way as for TLSv1.2 session.

The text of this International Standard is based on the following documents:

Draft	Report on voting
57/2578/FDIS	57/2593/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

- Abstract Syntax Notation One (ASN.1) are presented in `courier new` and **`bold courier new`**

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

IMPORTANT – The "colour inside" logo on the cover page of this document 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

This edition of IEC 62351-3 is a self-contained document profiling the usage of TLS for to secure power system communication. It is recommended to refer to this edition of this document rather than any previous edition, because this edition updates the utilized cryptographic algorithms (ciphersuites), provides enhanced functionality, and covers different TLS versions. In contrast to previous editions, this document specifies all necessary TLS specific settings and does not require the referencing standard to define specific settings for TLS.

Note that the recommendation to use this edition, potentially also with older referencing standards, requires technical support by implementations of the TLS settings specified in this edition of the document.

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 protocols that make use of TCP/IP as a message transport layer and utilize Transport Layer Security when cyber-security is required. This may relate to SCADA/telecontrol, protection, automation and control protocols.

IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (TLSv1.2 defined in RFC 5246, TLSv1.3 defined in RFC 8446). In the specific clauses, there will be subclauses to note the differences and commonalities in the application depending on the target TLS version. The use and specification of intervening external security devices (e.g., "bump-in-the-wire") are considered out-of-scope.

In contrast to previous editions of this document, this edition is self-contained in terms of completely defining a profile of TLS. Hence, it can be applied directly, without the need to specify further TLS parameters, except the port number, over which the communication will be performed. Therefore, this part can be directly utilized from a referencing standard and can be combined with further security measures on other layers. Providing the profiling of TLS without the need for further specifying TLS parameters allows declaring conformity to the described functionality without the need to involve further IEC 62351 documents.

This document is intended to be referenced as a normative part of other IEC standards that have the need for providing security for their TCP/IP-based protocol exchanges under similar boundary conditions. However, it is up to the individual protocol security initiatives to decide if this document is to be referenced.

The document also defines security events for specific conditions, which support error handling, security audit trails, intrusion detection, and conformance testing. Any action of an organization in response to events to an error condition described in this document are beyond the scope of this document and are expected to be defined by the organization’s security policy.

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

1.2 Intended audience

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

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

Portions of this document 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 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 62351-1:2007, *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 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

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

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 5288:2008, *AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289:2008, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

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

RFC 6066:2011, *Transport Layer Security Extensions*

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

RFC 8422:2018, *ECC Cipher Suites for TLSv1.2 and earlier*

RFC 8446:2018, *The TLS Protocol Version 1.3*

RFC 9150:2021, *TLS 1.3 Authentication and Integrity only Cipher Suites*

---

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

SOMMAIRE

AVANT-PROPOS 53
INTRODUCTION 55
1 Domaine d'application 56
1.1 Domaine d'application 56
1.2 Public ciblé 56
2 Références normatives 57
3 Termes, définitions et abréviations 58
3.1 Termes et définitions 58
3.2 Abréviations 58
4 Problèmes de sécurité couverts par le présent document 59
4.1 Généralités 59
4.2 Menaces à la sécurité contrées 59
4.3 Méthodes d'attaque contrées 60
4.4 Gestion des événements de sécurité 60
5 Vue d'ensemble des différences entre les versions TLS 61
5.1 Généralités 61
5.2 Principales différences entre TLSv1.2 et TLSv1.3 61
5.3 Nommage d'une suite chiffrée 62
5.4 Rétrocompatibilité 63
5.5 Extensions 63
6 Exigences génériques 64
6.1 Généralités 64
6.2 Signalisation des versions TLS prises en charge 64
6.3 Utilisation de suites chiffrées sans chiffrement 65
6.4 Prise en charge des certificats 66
6.4.1 Prise en charge d'ancres de confiance multiples 66
6.4.2 Taille de certificat 66
6.4.3 Échange de certificats 66
6.4.4 Validation des certificats de clé publique 67
6.5 Coexistence avec un trafic de protocole non sécurisé 70
7 Exigences spécifiques à TLSv1.2 71
7.1 Généralités 71
7.2 Suites chiffrées prises en charge 71
7.3 Suites chiffrées non autorisées 71
7.4 Échange de clés 72
7.4.1 Généralités 72
7.4.2 Mécanismes d'échange de clés 72
7.4.3 Algorithmes cryptographiques 72
7.4.4 Reprise de session 74
7.4.5 Renégociation de session 75
7.5 Prise en charge des extensions 76
7.5.1 Généralités 76
7.5.2 Extension de la renégociation de session TLS 76
7.5.3 Signalisation des certificats de CA pris en charge par le client par l'intermédiaire d'une CA de confiance 77
7.5.4 Signalisation des algorithmes de signature pris en charge 78

7.5.5 Agrafage des messages de réponse OCSP 79
7.5.6 Signalisation du serveur TLS cible prévu par l'indication du nom de serveur 80
7.5.7 Prise en charge du chiffrement avant authentification 80
8 Exigences spécifiques à TLSv1.3 80
8.1 Généralités 80
8.2 Suites chiffrées prises en charge 80
8.3 Échange de clés 81
8.3.1 Généralités 81
8.3.2 Modes d'établissement de liaison 82
8.3.3 Groupes Diffie-Hellman 83
8.3.4 Algorithmes de signature 83
8.4 Mise à jour des clés de session (message post-établissement de liaison) 85
8.5 Nouveau ticket de session (message de post-établissement de liaison) 85
8.6 Reprise de session 85
8.7 Validation de certificat 86
8.8 Prise en charge des extensions 86
8.8.1 Généralités 86
8.8.2 Signalisation des versions TLS prises en charge 86
8.8.3 Témoin de connexion 87
8.8.4 Signalisation des algorithmes de signature pris en charge 87
8.8.5 Signalisation des groupes pris en charge 87
8.8.6 Signalisation du partage de clés 88
8.8.7 Signalisation du serveur TLS cible prévu par l'indication du nom de serveur 88
8.8.8 Signalisation des autorités de certification prises en charge 88
8.8.9 Prise en charge de l'accord de clé basé sur PSK 89
8.8.10 Agrafage des messages de réponse OCSP 89
8.8.11 Signalisation des données précoces 89
9 Prise en charge de mesures de sécurité facultatives 90
10 Conformité 90
10.1 Généralités 90
10.2 Notation 90
10.3 Conformité aux versions TLS sélectionnées 90
10.4 Conformité à la gestion des certificats 91
10.5 Conformité aux spécifications de TLSv1.2 91
10.5.1 Conformité aux suites chiffrées sélectionnées 91
10.5.2 Conformité à la prise en charge des algorithmes cryptographiques 92
10.5.3 Conformité aux caractéristiques de gestion de session dans TLSv1.2 92
10.5.4 Conformité aux extensions sélectionnées dans TLSv1.2 93
10.6 Conformité aux spécifications de TLSv1.3 93
10.6.1 Conformité aux suites chiffrées sélectionnées dans TLSv1.3 93
10.6.2 Conformité aux caractéristiques de gestion de session sélectionnées dans TLSv1.3 94
10.6.3 Conformité aux extensions sélectionnées dans TLSv1.3 96
10.6.4 Conformité aux messages de post-établissement de liaison sélectionnés dans TLSv1.3 97
Annex A (informative) Événements de sécurité 98
A.1 Journaux d'événements de sécurité 98

A.2 Correspondance des événements TLS liés à l'établissement de liaison TLS 98
A.3 Correspondance des événements TLS liés à la gestion des certificats 100
Bibliographie 102

Figure 1 – Définition de suites chiffrées selon TLSv1.2 (RFC 5246) 62
Figure 2 – Définition des suites chiffrées selon TLSv1.3 (RFC 8446) 63

Tableau 1 – Prise en charge des suites chiffrées pour TLSv1.2 71
Tableau 2 – Prise en charge des suites chiffrées pour TLSv1.3 81
Tableau 3 – Prise en charge des modes d'établissement de liaison basés sur PSK pour TLSv1.3 82
Tableau 4 – Prise en charge des groupes Diffie-Hellman pour TLSv1.3 83
Tableau 5 – Algorithmes de signature pris en charge pour l'établissement de liaison dans TLSv1.3 84
Tableau 6 – Algorithmes de signature pris en charge pour les certificats dans TLSv1.3 84
Tableau 7 – Conformité aux versions TLS 91
Tableau 8 – Conformité à la prise en charge des certificats 91
Tableau 9 – Conformité aux suites chiffrées utilisables avec TLSv1.2 92
Tableau 10 – Conformité à la prise en charge des algorithmes cryptographiques 92
Tableau 11 – Conformité aux caractéristiques de gestion de session dans TLSv1.2 93
Tableau 12 – Conformité aux extensions d'établissement de liaison dans TLSv1.2 93
Tableau 13 – Conformité aux suites chiffrées dans TLSv1.3 94
Tableau 14 – Conformité aux modes d'établissement de TLSv1.3 94
Tableau 15 – Conformité à la caractéristique de données précoces (0-RTT) de TLSv1.3 94
Tableau 16 – Conformité aux groupes Diffie-Hellman pris en charge dans TLSv1.3 95
Tableau 17 – Conformité aux algorithmes de signature pris en charge pour l'établissement de liaison dans TLSv1.3 95
Tableau 18 – Conformité aux algorithmes de signature pris en charge pour les certificats dans TLSv1.3 96
Tableau 19 – Conformité aux extensions dans TLSv1.3 96
Tableau 20 – Conformité aux messages de post-établissement de liaison dans TLSv1.3 97
Tableau A.1 – Correspondance entre les journaux d'événements de sécurité liés à l'établissement de liaison TLS définis dans l'IEC 62351-3:— (Éd.2) et l'IEC 62351-14 98
Tableau A.2 – Correspondance entre les journaux d'événements de sécurité liés à la validation des certificats définis dans l'IEC 62351-3 Éd.2 et l'IEC 62351-14 100

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 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 propriété et averti de leur existence.

L'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. Il s'agit d'une Norme internationale.

Cette seconde édition annule et remplace la première édition parue en 2014, l'Amendement 1:2018 et l'Amendement 2:2020. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) inclusion du paramètre lié à la TLSv1.2 exigé dans l'IEC 62351-3 Éd.1.2 à spécifier par la norme de référence. Ce paramètre comprend les éléments suivants:

- les suites chiffrées TLSv1.2 obligatoires à prendre en charge;
- la spécification des paramètres de reprise de session;
- la spécification des paramètres de renégociation de session;
- la gestion des révocations à l'aide de la CRL et du protocole OCSP;
- la gestion des événements de sécurité;

b) inclusion d'un profil TLSv1.3 applicable au domaine des systèmes de puissance d'une manière similaire à celle de la session TLSv1.2.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2578/FDIS	57/2593/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

NOTE Les caractères d'imprimerie suivants sont employés:

- les caractères en notation de syntaxe abstraite numéro un (ASN.1) sont présentés en `courier new` et **`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*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera:

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document 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

La présente édition de l'IEC 62351-3 est un document autosuffisant qui décrit l'utilisation de la TLS pour sécuriser la communication des systèmes de puissance. Il est recommandé de se référer à la présente édition du présent document plutôt qu'à n'importe quelle édition précédente, car cette édition met à jour les algorithmes cryptographiques utilisés (suites chiffrées, en anglais cipher suites), fournit des fonctionnalités améliorées et couvre différentes versions TLS. Contrairement aux éditions précédentes, le présent document spécifie tous les réglages spécifiques TLS nécessaires et n'exige pas que la norme de référence définisse des réglages spécifiques pour la TLS.

Il est à noter que la recommandation d'utiliser la présente édition, éventuellement aussi avec des normes de référencement plus anciennes, exige un support technique par les mises en œuvre des paramètres TLS spécifiés dans la présente édition du document.

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 assurer la confidentialité, la protection de l'intégrité et l'authentification des niveaux des messages pour les protocoles qui utilisent les protocoles TCP/IP comme couche transport des messages et utilisent la sécurité de la couche transport lorsque la cybersécurité est exigée. Ceci peut concerner les protocoles SCADA/téléconduite, protection, automation et contrôles.

L'IEC 62351-3 spécifie une méthode permettant de sécuriser les protocoles TCP/IP par l'intermédiaire de contraintes sur la spécification des messages, procédures et algorithmes de sécurité de la couche transport (TLS) (version 1.2 de TLS définie dans la RFC 5246 et version 1.3 définie dans la RFC 8446). Des articles spécifiques contiennent des paragraphes indiquant les différences et les points communs d'application en fonction de la version TLS cible. 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 du présent document.

Contrairement aux précédentes éditions du présent document, la présente édition est autosuffisante, car elle définit entièrement un profil de TLS. De ce fait, elle peut être appliquée directement, sans nécessiter de spécifier de paramètres TLS supplémentaires, à l'exception du numéro du port par lequel la communication est effectuée. Par conséquent, la présente partie peut être directement utilisée à partir d'une norme de référence et peut être combinée avec des mesures de sécurité supplémentaires sur d'autres couches. La définition du profil de TLS sans nécessiter de spécifier de paramètres TLS supplémentaires permet de déclarer la conformité à la fonctionnalité décrite sans nécessiter de recourir à d'autres documents IEC 62351.

Le présent document est destiné à être référencé comme partie normative des autres normes IEC qui traitent de la nécessité d'assurer la sécurité de leurs échanges protocolaires basés sur TCP/IP dans des conditions limites similaires. Cependant, il revient aux initiatives individuelles en matière de sécurité des protocoles de décider si le présent document est à référencer.

Le présent document définit également des événements de sécurité pour des conditions spécifiques, qui prennent en charge la gestion des erreurs, les pistes d'audit de sécurité, la détection d'intrusion et les essais de conformité. Toute action d'un organisme en réponse à des événements dus à une condition d'erreur décrite dans le présent document ne relève pas du domaine d'application du présent document et est susceptible d'être définie par la politique de sécurité de l'organisme.

Le présent document présente les exigences de sécurité des protocoles de gestion des systèmes de puissance de l'IEC. Une révision du présent document pourrait s'avérer nécessaire en cas d'ajout de nouvelles exigences dans d'autres normes.

1.2 Public ciblé

Les premiers utilisateurs auxquels s'adresse le présent document sont les experts qui développent ou utilisent les protocoles dans le domaine de la gestion des systèmes de

puissance et des échanges d'informations associés. Pour que les mesures décrites dans le présent document prennent effet, elles doivent être acceptées et référencées par les spécifications de protocoles qui utilisent la sécurité TCP/IP en appliquant la TLS. Le présent document est rédigé afin de permettre ce processus.

Les autres utilisateurs auxquels s'adresse le présent document sont les développeurs de produits qui mettent en œuvre ces protocoles.

Des parties du présent document peuvent également être utiles aux responsables et aux dirigeants afin de comprendre l'objectif d'une activité et les exigences correspondantes.

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 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 62351-9, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance*

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

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 5288:2008, *AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289:2008, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

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

RFC 6066:2011, *Transport Layer Security Extensions*

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

RFC 8422:2018, *ECC Cipher Suites for TLSv1.2 and earlier*

RFC 8446:2018, *The TLS Protocol Version 1.3*

_____

[1] Généralement appelé SSL/TLS.

RFC 9150:2021, *TLS 1.3 Authentication and Integrity only Cipher Suites*