

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 2 AMENDEMENT 2

**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22,000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67,000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 2 AMENDEMENT 2

**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 978-2-8322-7713-3

**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.**

FOREWORD

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

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

FDIS	Report on voting
57/2149/FDIS	57/2167/RVD

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
<https://standards.iteh.ai/catalog/standards/sist/4c101d57-06ed-474a-bed9-344b29e1efb5/iec-62351-3-2014-amd2-2020>

INTRODUCTION to Amendment 2

This amendment to International Standard IEC 62351-3 and its Amendment 1 (2018) 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.

2 Normative references

Add the following new document to the list of references:

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

4 Security issues addressed by this standard

4.2 Security threats countered

Replace the existing text of the second paragraph of Subclause 4.2 as modified by Amendment 1 with the following new text:

TCP/IP and the security specifications in this part of IEC 62351 cover only the communication transport layers (OSI layers 4 and lower). Specifically, TLS protects the transported messages from OSI layer 5 and above in a transparent way. This part of IEC 62351 does not cover security functionality specific for the communication application layers (OSI layers 5 and above) or application-to-application security.

Add, after existing Subclause 4.3 as modified by Amendment 1, the following new Subclause 4.4:

(standards.iteh.ai)

4.4 Handling of security events

Throughout the document security events are defined as warnings and alarms. These security events are intended to support the error handling and thus to increase system resilience. Implementations should provide a mechanism for announcing security events.

It is recommended that the security warning and alarms throughout the document are implemented by cyber security events as specified by IEC 62351-14 or by monitoring objects as specified by IEC 62351-7.

Note that warnings and alarms are used to indicate the severity of an event from a security point of view. The following notion is used:

- A warning was intended to raise awareness but to indicate that it may be safe to proceed.
- An alarm is an indication to not proceed.

In any case, it is expected that an operator's security policy determines the final handling based on the operational environment.

5 Mandatory requirements

5.1 Deprecation of cipher suites

Replace the existing text of the second paragraph of Subclause 5.1 with the following new text:

If the communication connection is encrypted the following cipher suites may be used:

- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256

Replace the existing text of the fourth paragraph of Subclause 5.1 as added by Amendment 1 with the following new text:

The support of SHA-1 is deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash algorithm to be used.

Add, at the end of Subclause 5.1, the following new text:

The failure in finding a matching cipher suite during the TLS handshake shall raise a security event ("alarm: no matching TLS cipher suites").

5.2 Negotiation of versions

Replace the existing text of the first paragraph of Subclause 5.2 with the following new text:

TLS v1.2 as defined in RFC 5246 (sometimes referred to as SSL v3.3) is the default version that shall be supported. Higher versions may be supported.

NOTE 1 This document refers to features defined for TLS 1.2. Higher versions of TLS, like TLS 1.3, do not necessarily support all features listed in this document.

It is recommended that the TLS client initiating a TLS connection indicates the highest TLS version supported in the `ClientHello` message of the TLS handshake. The receiving TLS server may accept higher versions if functional supported and allowed by the security policy of the operating environment.

To ensure backward compatibility implementations may optionally support TLS version 1.0 and 1.1 (sometimes referred to as SSL v3.1 and v3.2). The TLS handshake provides a built-in mechanism that shall be used to support version negotiation. The peer initiating a TLS connection shall always indicate the highest TLS version supported during the TLS handshake message. The application of TLS versions other than v1.2 is a matter of the local security policy. Proposal of versions prior to TLS 1.0 shall result in no secure connection being established (see also RFC 6176).

NOTE 2 For TLS 1.0 and TLS 1.1 certain security issues are known, The optional support is only intended for backward compatibility and it is strongly recommended to switch to TLS 1.2.

Replace the existing text of the second and third paragraphs of Subclause 5.2 with the following new text:

The proposal of versions prior to TLS 1.0 or SSL 3.1 shall raise a security event ("alarm: unsecure communication").

NOTE 3 The option to remotely monitor security events is preferred.

The proposal of versions TLS 1.0 or TLS 1.1 shall raise a security event ("warning: insecure TLS version").

Add, at the end of Subclause 5.2, the following new text:

If the negotiated TLS version from the initial TLS handshake changes in an ongoing TLS session during a TLS session renegotiation or a session resumption handshake from either side the TLS session shall be terminated. The termination of the session should raise a security event ("alarm: TLS Version change detected").

5.3 Session Resumption

Replace the reference to RFC 5280 in the first paragraph of Subclause 5.3 as modified by Amendment 1 with the following new reference:

RFC 5246

Replace the last sentence of the first paragraph of Subclause 5.3 as modified by Amendment 1 with the following new text:

Session resumption is expected to be more frequent than session renegotiation leading to a smaller session resumption interval than the session renegotiation interval. ($0 < \text{session resumption interval} < \text{session renegotiation interval} \leq 24\text{h}$).

Replace the reference to PIXIT in the second paragraph of Subclause 5.3 as modified by Amendment 1 with the following new reference:

PICS

At the end of Subclause 5.3 as modified by Amendment 1 add the following note:

NOTE An informative example regarding the configuration is provided at the end of Subclause 5.4.

5.4 Session renegotiation

Replace the reference to "PIXIT (Protocol Implementation eXtra Information for Testing)" in the third paragraph of Subclause 5.4 as modified by Amendment 1 with the following new reference:

PICS

Replace the existing text of the sixth paragraph of Subclause 5.4 as added by Amendment 1 with the following new text:

The calling (TLS client) and the called (TLS server) entity are responsible for verifying that the TLS session renegotiation takes place at the expected intervals. If the calling entity does not receive a TLS session renegotiation request (`HelloRequest`) from the called entity at the expected interval, then the calling entity shall initiate the TLS renegotiation itself using a `ClientHello`. If the called entity does not receive a TLS renegotiation (`ClientHello`) in response to a `HelloRequest`, the called entity shall terminate the connection. The termination of a connection due to a missed TLS session renegotiation should raise a security event ("alarm: session renegotiation interval expired").

Add the following new text at the end of Subclause 5.4:

The following Informative example is provided:

- The assumed CRL refresh time (or OCSP response validity) is 24h.
- Session renegotiation involves the validation of the peer certificates including the revocation check. Session renegotiation involving the peer certificates for authentication may be performed at least every 12 hours.
- To allow for a session key update during the 12-hour session renegotiation interval session resumption is performed every 2 hours during the session. The maximum time to resume a previously ended session is 24 hours.

5.6.1 Multiple Certification Authorities (CAs)

Replace the existing text of the last paragraph of Subclause 5.6.1 with the following new text:

The failure of selecting a matching CA issued certificate shall raise a security event ("alarm: CA certificate not found").

5.6.2 Certificate size

Add, at the end of Subclause 5.6.2, the following new text:

Exceeding the maximum size of a certificate during a TLS handshake shall raise a security event ("alarm: TLS certificate size exceeded").

5.6.3 Certificate exchange

Replace the existing text of the last paragraph of Subclause 5.6.3 as modified by Amendment 1 with the following new text:

The connection termination due to the lack of a certificate of either side shall raise a security event ("alarm: certificate unavailable").

5.6.4.2 Verification based upon CA

Add, at the end of Subclause 5.6.4.2, the following new text:

The failure of finding a matching CA certificate during a TLS handshake shall raise a security event ("alarm: certificate validation: CA certificate not available").

5.6.4.3 Verification based upon individual certificates

Add, at the end of Subclause 5.6.4.3, the following new text:

The failure of finding a matching individual certificate during a TLS handshake shall raise a security event ("alarm: certificate validation: trusted individual certificate not available").

5.6.4.4 Certificate revocation

Add, after the fourth paragraph of Subclause 5.6.4.4 as modified by Amendment 1, the following new text:

<https://standards.iteh.ai/catalog/standards/sist/4c101d57-06ed-474a-bed9-344b291def5/iec-62351-3-2014-amd2-2020>

The unavailability of a CRL shall raise a security event ("warning: CRL not accessible").

NOTE 1 The CRL may be distributed in different ways (manual as file, fetched from CRL distribution point, etc.).

NOTE 2 If there are no revoked certificates, the CRL is an empty list, but still needs to be available."

The expiry of a CRL shall raise a security event ("warning: CRL expired")."

If OCSP is applied for certificate revocation checks, the inaccessibility to the OCSP responder shall raise a security event: ("warning: OCSP responder not accessible"). The expiry of an OCSP response shall raise a security event ("warning: OCSP response expired")."

Replace the existing text of the last paragraph of Subclause 5.6.4.4 as modified by Amendment 1 with the following new text:

The refusal / termination of a connection due to a revoked certificate shall raise a security event ("alarm: revoked certificate").

Renumber the existing note at the end of Subclause 5.6.4.4 as modified by Amendment 1 as NOTE 3.

5.6.4.5 Expired certificates

Replace the existing text of the last paragraph of Subclause 5.6.4.5 as modified by Amendment 1 with the following new text:

The refusal of a connection due to an expired certificate shall raise a security event ("alarm: expired certificate").

5.6.4.6 Signing

Delete the following bullet point in the second paragraph of Subclause 5.6.4.6:

- Optional: Signature-operation: RSA with a key length of 1 024 Bits (legacy mode);

Delete the following text from the second bullet point in the second paragraph of Subclause 5.6.4.6:

(modern mode)

Replace the existing text of the third paragraph of Subclause 5.6.4.6 with the following new text:

The support of RSA with 1 024 bit keys is deprecated. Its use is limited to backward compatibility. RSA with 2 048 bit keys must be supported and is the preferred signature algorithm to be used.

Replace the existing text of the ninth paragraph of Subclause 5.6.4.6 as added by Amendment 1 with the following new text:

The support of SHA-1 is deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash algorithm to be used.

Add, at the end of Subclause 5.6.4.6, the following new text:

The failure of finding a matching signature algorithm to the certificate components during a TLS handshake shall raise a security event ("alarm: certificate validation: algorithms not supported").

The failure of validating the signature of received certificate during a TLS handshake shall raise a security event ("alarm: certificate validation: certificate signature could not be validated").

5.6.4.7 Key Exchange

Delete the following bullet point in the first paragraph of Subclause 5.6.4.7 as modified by Amendment 1:

- Optional: Signature-operation: RSA with a key length of 1 024 Bits (legacy mode);

Delete the following text from the second bullet point in the first paragraph of Subclause 5.6.4.7 as modified by Amendment 1:

(modern mode)

Replace the existing text of the second paragraph of Subclause 5.6.4.7 as modified by Amendment 1 with the following new text:

The support of RSA with 1 024 bit keys is deprecated. Its use is limited to backward compatibility. RSA with 2 048 bit keys must be supported and is the preferred signature algorithm to be used. The detection of RSA keys with 1024 Bit shall raise a security event ("warning: minimum key length"). The detection of RSA keys with less than 1 024 Bit shall raise a security event ("alarm: insufficient key length").

Replace the existing text of the seventh paragraph of Subclause 5.6.4.7 with the following new text:

The support of SHA-1 is deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash algorithm to be used.

7 Referencing standard requirements

Add the following new bullet after the first bullet point of Clause 7 as modified by Amendment 1:

- If other versions than TLS 1.2 are to be used, the referencing standard shall define the required versions.

8 Conformance

Replace the existing text of Article 8 with the following new text:

8.1 General

Static conformance requirements specify what shall be implemented, what may be implemented and what shall not be implemented for an implementation claiming compliance to this document.

Note that this section only refers to settings defined in Clause 5. The referencing standard will provide further TLS related PICS statements in addition or as specification of an optional requirement.

8.2 Notation

The following notations are used for specifying conformance requirements:

- m: Mandatory support. The item shall be implemented.
- o: Optional support. The item may be, but need not be implemented.
- x: Excluded. The item shall not be supported.

8.3 Conformance to selected cipher suites

Table 1 states the conformance requirements for TLS cipher suites, which are defined in Subclause 5.1.

Table 1 – Conformance to TLS cipher suites

Cipher suite	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
TLS_NULL_WITH_NULL_NULL	x		x		
TLS_RSA_WITH_NULL_MD5	x		x		
TLS_RSA_WITH_NULL_SHA	o		o		SHA-1 deprecated
TLS_RSA_WITH_NULL_SHA256	o		o		

Note that Subclause 5.1 also allows other cipher suites for integrity only support. Moreover, specific cipher suites considered mandatory or optional will be specified by the referencing standard.

8.4 Conformance to selected TLS versions

Table 2 states the conformance requirements for TLS version, which are defined in Subclause 5.2.

Table 2 – Conformance to TLS versions

TLS Version	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
1.0	o		o		Weaknesses known, only for backward compatibility
1.1	o		o		Weaknesses known, only for backward compatibility
1.2	m		m		
1.3	o		o		Not all features specified in this document

8.5 Conformance to selected TLS protocol features

Table 3 states the conformance requirements for TLS version, which are defined in Subclauses 5.3, 5.4, and 5.6.

Table 3 – Conformance to TLS protocol features

TLS feature	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
TLS Session resumption at least every 24 hours	m		m		
TLS Session resumption initiation using ClientHello	m		x		
TLS Session resumption initiation using HelloRequest	x		m		
TLS Session resumption using session tickets	o		o		according to RFC 5077
TLS Session renegotiation at least every 24 hours	m		m		
TLS Session renegotiation initiation using ClientHello	m		x		
TLS Session renegotiation initiation using HelloRequest	x		m		
TLS Session renegotiation extension	m		m		according to RFC 5746
Support of trusted CA extension (RFC 6066)	o		o		

8.6 Conformance to certificate support

Table 4 states the conformance requirements for certificate support, which are defined in Subclause 5.6 and Clause 6.

Table 4 – Conformance to certificate support

	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
Support of multiple CA (root certificates)	o		o		Referencing standard defined.
Maximum supported certificate size is 8 192 bytes	m		m		<i>To be discussed?</i>
Follow certificate validation rules according to RFC 5280 (validity, CA signature, revocation state, etc.)	m		m		
Certificate revocation state validation using CRL	m		m		Evaluation period to be specified by the referencing standard.
Certificate revocation state validation using OCSP	o		o		
Certificate white listing according to IEC 62351-9	o		o		