IEC 62351-3

Edition 1.0 2020-02

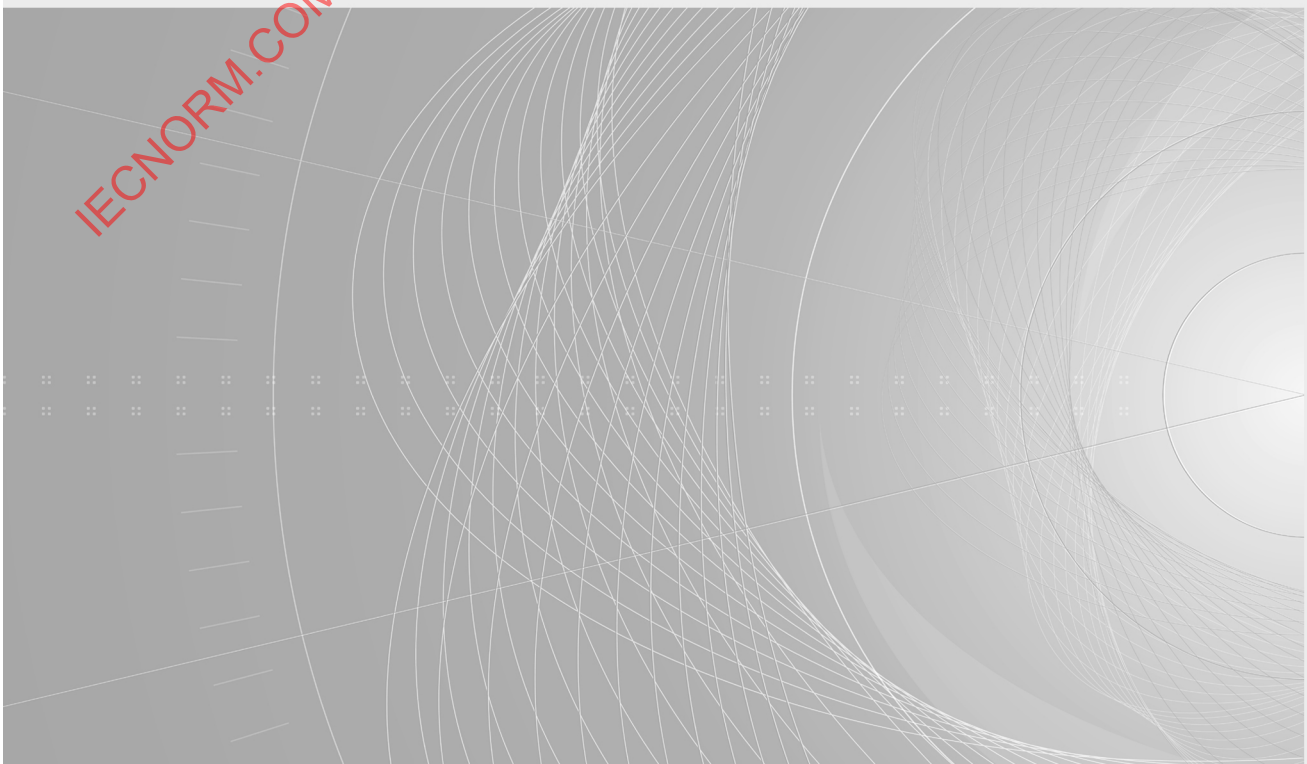
INTERNATIONAL STANDARD

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



IEC 62351-3:2014-10/AMD2:2020-02(en-fr)

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

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

IEC 62351-3

Edition 1.0 2020-02

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

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.

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:

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 < session resumption interval < session renegotiation interval <= 24h).

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:

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 oar 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		*To be discussed?*
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		

8.7 Conformance to cryptographic algorithm support

Table 5 states the conformance requirements for certificate support, which are defined in Subclauses 5.6.4.6 and 5.6.4.7.

Table 5 – Conformance to cryptographic algorithm support

Signature and Hash algorithms	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
Support of RSA 2048	m		m		
Support of RSA 1024	o		o		deprecated
Support of ECDSA with 256 bit keys, OID: 1.2.840.10045.4.3.2; Support of curve secp256r1, OID: 1.2.840.10045.3.1.7	o		o		
Support of ECGDSA with 256 bit keys, OID: 1.3.36.3.3.2.5.4.4; Support of curve brainpoolP256r1, OID: 1.3.36.3.3.2.8.1.1.7	o		o		
Support of SHA-256	m		m		
Support of SHA-1	o		o		deprecated
Support of MD5	x		x		

Bibliography

add the following new documents to the bibliography:

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 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Events Logs*[1]

[1] Under preparation. Stage at the time of publication: IEC/PCC 62351-14:2020.

AVANT-PROPOS

Le présent amendement à la Norme internationale IEC 62351-3 a été établi par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
57/2149/FDIS	57/2167/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de la présente norme.

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 cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION à l'Amendement 2

Le présent amendement à la Norme internationale IEC 62351-3 et son Amendement 1 (2018) 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.

2 Références normatives

Ajouter le nouveau document suivant à la lise des références:

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)

4 Problèmes de sécurité couverts par la présente norme

4.2 Menaces à la sécurité contrées

Remplacer le texte existant du deuxième alinéa de 4.2, modifié par l'Amendement 1, par le nouveau texte suivant:

Les protocoles TCP/IP et les spécifications de sécurité dans la présente partie de l'IEC 62351 couvrent uniquement les couches transport de communication (couches OSI 4 et inférieures). Plus précisément, la TLS protège de manière transparente les messages transportés de la couche OSI 5 et supérieure. La présente partie de l'IEC 62351 ne couvre pas la fonctionnalité de sécurité spécifique aux couches application de communication (couches OSI 5 et supérieures) ou la sécurité d'application à application.

Ajouter, après le Paragraphe 4.3 existant, modifié par l'Amendement 1, le nouveau Paragraphe 4.4 suivant:

4.4 Gestion des événements de sécurité

Dans l'ensemble du document, les événements de sécurité sont définis comme des avertissements et des alarmes. Ces événements de sécurité sont destinés à prendre en charge la gestion des erreurs et donc à accroître la résilience du système. Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.

Il est recommandé que les avertissements et alarmes de sécurité contenus dans le document soient mis en œuvre par les événements de cybersécurité spécifiés dans l'IEC 62351-14 ou par les objets de surveillance spécifiés dans l'IEC 62351-7.

Noter que les avertissements et les alarmes servent à indiquer la gravité d'un événement en matière de sécurité. La notion suivante est utilisée:

– Un avertissement a pour but de sensibiliser le public, et d'indiquer qu'il peut continuer en toute sécurité.
– Une alarme est une indication de ne pas continuer.

Dans tous les cas, il est prévu que la politique de sécurité de l'opérateur détermine le traitement final en fonction de l'environnement d'exploitation.

5 Exigences obligatoires

5.1 Rejet de suites chiffrées

Remplacer le texte existant du deuxième alinéa de 5.1 de l'Amendment 1 par le nouveau texte suivant

Si la connexion de communication est chiffrée, les suites chiffrées suivantes peuvent être utilisées:

– TLS_RSA_WITH_NULL_SHA
– TLS_RSA_WITH_NULL_SHA256

Remplacer le texte existant du quatrième alinéa de 5.1, ajouté par l'Amendement 1, par le nouveau texte suivant:

La prise en charge de SHA-1 est déconseillée. Son utilisation est limitée à la rétrocompatibilité. SHA-256 doit être pris en charge et représente l'algorithme de hachage préférentiel à utiliser.

Ajouter, à la fin de 5.1, le nouveau texte suivant:

L'échec de sélection d'une suite chiffrée correspondante au cours du protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: aucune suite chiffrée TLS correspondante").

5.2 Négociation des versions

Remplacer le texte existant du premier alinéa de 5.2 par le nouveau texte suivant:

La TLS v1.2 telle que définie dans la RFC 5246 (parfois appelée SSL v3.3) est la version par défaut qui doit être prise en charge. Des versions supérieures peuvent être prises en charge.

NOTE 1 Le présent document fait référence aux caractéristiques définies pour la TLS 1.2. Des versions TLS supérieures telles que TLS 1.3 ne prennent pas nécessairement en charge toutes les caractéristiques définies dans le présent document.

Il est recommandé que le client TLS initiant une connexion TLS indique la version TLS la plus élevée prise en charge dans le message `ClientHello` du protocole de transfert TLS. Le serveur TLS récepteur peut admettre des versions supérieures si elles sont fonctionnelles, prises en charge et autorisées par la politique de sécurité de l'environnement d'exploitation.

Pour garantir la rétrocompatibilité, les mises en œuvre peuvent éventuellement prendre en charge les versions 1.0 et 1.1 de TLS (parfois appelées SSL v3.1 et v3.2). Le protocole de transfert TLS fournit un mécanisme intégré qui doit être utilisé pour prendre en charge la négociation de la version. L'homologue initiant une connexion TLS doit toujours indiquer la version TLS la plus élevée prise en charge pendant le message de protocole de transfert TLS. L'application de versions TLS autres que v1.2 relève de la politique de sécurité locale. La proposition de versions inférieures à TLS 1.0 ne doit pas provoquer l'établissement d'une connexion sécurisée (voir aussi la RFC 6176).

NOTE 2 Certains problèmes de sécurité sont identifiés au niveau des versions TLS 1.0 et TLS 1.1. La prise en charge facultative est uniquement destinée à la rétrocompatibilité et il est vivement recommandé de passer à la TLS 1.2.

Remplacer le texte existant des deuxième et troisième alinéas de 5.2 par le nouveau texte suivant:

La proposition de versions inférieures à TLS 1.0 ou SSL 3.1 doit entraîner un événement de sécurité ("alarme: communication non sécurisée").

NOTE 3 L'option consistant à contrôler les événements de sécurité à distance est préférentielle.

La proposition de versions TLS 1.0 ou TLS 1.1 doit entraîner un événement de sécurité ("avertissement: version TLS non sécurisée").

Ajouter, à la fin de 5.2, le nouveau texte suivant:

Si la version TLS négociée à partir du protocole initial de transfert TLS change dans une session TLS en cours lors d'une renégociation de session TLS ou d'un protocole de transfert de reprise de session d'un côté ou de l'autre, la session TLS doit être terminée. Il convient que l'arrêt de la session entraîne un événement de sécurité ("alarme: changement de version TLS détecté").

5.3 Reprise de session

Remplacer la référence à RFC 5280 dans le premier alinéa de 5.3, modifié par l'Amendement 1, par la nouvelle référence suivante;

RFC 5246

Remplacer la dernière phrase du premier alinéa de 5.3, modifié par l'Amendement 1, par le nouveau texte suivant:

Il est prévu que la reprise de session soit plus fréquente que la renégociation de session, ce qui entraîne un intervalle de reprise de session plus petit que l'intervalle de renégociation de session. (0 < intervalle de reprise de session < intervalle de renégociation de session <= 24 h).

Remplacer la référence à PIXIT, dans le deuxième alinéa de 5.3, modifié par l'Amendement 1, par la nouvelle référence suivante:

PICS

À la fin de 5.3, modifié par l'Amendement 1, ajouter la note suivante:

NOTE Un exemple informatif concernant la configuration est donné à la fin de 5.4.

5.4 Renégociation de session

Remplacer la référence à "PIXIT (Protocol Implementation eXtra Information for Testing)" au troisième alinéa de 5.4, modifié par l'Amendement 1, par la nouvelle référence suivante:

PICS

Remplacer le texte existant du sixième alinéa de 5.4, modifié par l'Amendement 1, par le nouveau texte suivant

L'entité appelante (client TLS) et l'entité appelée (serveur TLS) sont chargées de vérifier que la renégociation de la session TLS a lieu aux intervalles prévus. Si l'entité appelante ne reçoit pas de demande de renégociation de session TLS (`HelloRequest`) de la part de l'entité appelée aux intervalles prévus, l'entité appelante doit alors initier elle-même la renégociation de session TLS à l'aide d'un `ClientHello`. Si l'entité appelée ne reçoit pas un message de renégociation de session TLS (`ClientHello`) en réponse à un `HelloRequest`, l'entité appelée doit mettre fin à la connexion. Il convient que l'arrêt de la connexion dû à une renégociation de session TLS manquée entraîne un événement de sécurité ("alarme: intervalle de renégociation de session expiré").

À la fin de 5.4, ajouter le nouveau texte suivant:

L'exemple informatif suivant est fourni:

– Le temps estimé de rafraîchissement de la CRL (ou la validité de la réponse de l'OCSP) est de 24 h.
– La renégociation de session implique la validation de certificats homologues, dont la vérification de révocation. La renégociation de session impliquant les certificats homologues pour authentification peut être réalisée au moins toutes les 12 h.
– Afin de permettre une mise à jour clé de la session pendant l'intervalle de 12 h entre deux renégociations de sessions, une reprise de session est réalisée toutes les 2 h pendant la session. Le temps maximal accordé pour reprendre une session clôturée précédemment est de 24 h.

5.6.1 Autorités de certification multiples (CA, Certificate Authorities)

Remplacer le texte existant du dernier alinéa de 5.6.1 par le nouveau texte suivant:

L'échec de sélection d'un certificat correspondant émis par la CA doit entraîner un événement de sécurité ("alarme: certificat CA non trouvé").

5.6.2 Taille de certificat

Ajouter, à la fin de 5.6.2, le nouveau texte suivant:

Le dépassement de la taille maximale d'un certificat au cours d'un protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: taille du certificat TLS dépassée").

5.6.3 Échange de certificat

Remplacer le texte existant du dernier alinéa de 5.6.3, modifié par l'Amendement 1, par le nouveau texte suivant:

L'arrêt de la connexion dû à l'absence de certificat de l'un ou l'autre côté doit entraîner un événement de sécurité ("alarme: certificat non disponible").

5.6.4.2 Vérification basée sur la CA

Ajouter, à la fin de 5.6.4.2, le nouveau texte suivant:

L'échec de sélection d'un certificat CA correspondant au cours d'un protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: validation de certificat: certificat CA non disponible").

5.6.4.3 Vérification basée sur des certificats individuels

Ajouter, à la fin de 5.6.4.3, le nouveau texte suivant:

L'échec de sélection d'un certificat individuel correspondant au cours d'un protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: validation de certificat: certificat individuel de confiance non disponible").

5.6.4.4 Révocation de certificat

Ajouter, après le quatrième alinéa de 5.6.4.4, modifié par l'Amendement 1, le nouveau texte suivant:

L'indisponibilité d'une CRL doit entraîner un événement de sécurité ("avertissement: CRL non accessible").

NOTE 1 La CRL peut être diffusée de différentes manières (manuelle sous forme de fichier, par mise à disposition au niveau des points de distribution de CRL, etc.).

NOTE 2 Si aucun certificat n'est révoqué, la CRL est une liste vide, dont la disponibilité est toujours nécessaire.

L'expiration d'une CRL doit entraîner un événement de sécurité ("avertissement: CRL expirée").

Si un OCSP est utilisé pour les vérifications de révocation de certificat, l'inaccessibilité au répondeur OCSP doit entraîner un événement de sécurité: ("avertissement: répondeur OCSP non accessible"). L'expiration d'une réponse de l'OCSP doit entraîner un événement de sécurité ("avertissement: réponse OCSP expirée").

Remplacer le texte existant du dernier alinéa de 5.6.4.4, modifié par l'Amendement 1, par le nouveau texte suivant:

Le refus / l'arrêt d'une connexion dû à un certificat révoqué doit entraîner un événement de sécurité ("alarme: certificat révoqué").

Renuméroter la note existante à la fin de 5.6.4.4, modifié par l'Amendement 1, en NOTE 3.

5.6.4.5 Certificats expirés

Remplacer le texte existant du dernier alinéa de 5.6.4.5 par le nouveau texte suivant

Le refus d'une connexion dû à un certificat expiré doit entraîner un événement de sécurité ("alarme: certificat expiré").

5.6.4.6 Signature

Supprimer du deuxième alinéa de 5.6.4.6, modifié par l'Amendement 1, le tiret suivant:

– Facultative: Opération de signature: RSA d'une longueur de clé de 1 024 Bits (mode hérité);

Supprimer du deuxième alinéa, second tiret, de 5.6.4.6, le texte suivant:

(mode moderne)

Remplacer le texte existant du troisième alinéa de 5.6.4.6 par le nouveau texte suivant:

La prise en charge d'un RSA d'une longueur de clé de 1 024 bits est déconseillée. Son utilisation est limitée à la rétrocompatibilité. Le RSA d'une longueur de clé de 2 048 bits doit être pris en charge, et il représente l'algorithme de signature préférentiel à utiliser.

Remplacer le texte existant du neuvième alinéa de 5.6.4.6, ajouté par l'Amendement 1, par le nouveau texte suivant:

La prise en charge de SHA-1 est déconseillée. Son utilisation est limitée à la rétrocompatibilité. SHA-256 doit être pris en charge et représente l'algorithme de hachage préférentiel à utiliser.

Ajouter, à la fin de 5.6.4.6, le nouveau texte suivant:

L'échec de sélection d'un algorithme de signature correspondant aux composantes du certificat au cours d'un protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: validation de certificat: algorithmes non pris en charge").

L'échec de validation de la signature d'un certificat reçu au cours d'un protocole de transfert TLS doit entraîner un événement de sécurité ("alarme: validation de certificat: signature de certificat ne peut être validée").

5.6.4.7 Échange de clés

Supprimer du premier alinéa de 5.6.4.7, modifié par l'Amendement 1, le tiret suivant:

– Facultative: Opération de signature: RSA d'une longueur de clé de 1 024 Bits (mode hérité);

Supprimer du premier alinéa, second tiret, de 5.6.4.7, modifié par l'Amendement 1, le texte suivant:

(mode moderne)

Remplacer le texte existant du deuxième alinéa de 5.6.4.7, modifié par l'Amendement 1, par le nouveau texte suivant:

La prise en charge d'un RSA d'une longueur de clé de 1 024 bits est déconseillée. Son utilisation est limitée à la rétrocompatibilité. Le RSA d'une longueur de clé de 2 048 bits doit être pris en charge, et il représente l'algorithme de signature préférentiel à utiliser. La détection des clés RSA de 1 024 bits doit entraîner un événement de sécurité ("avertissement: longueur de clé minimale"). La détection des clés RSA de moins de 1 024 bits doit entraîner un événement de sécurité ("alarme: longueur de clé insuffisante").

Remplacer le texte existant du septième alinéa de 5.6.4.7 par le nouveau texte suivant:

La prise en charge de SHA-1 est déconseillée. Son utilisation est limitée à la rétrocompatibilité. SHA-256 doit être pris en charge et représente l'algorithme de hachage préférentiel à utiliser.

7 Exigences relatives aux normes de référence

Ajouter, après le premier tiret de l'Article 7, modifié par l'Amendement 1, le nouveau tiret suivant:

– Si des versions autres que la TLS 1.2 doivent être utilisées, la norme de référence doit définir les versions exigées.

8 Conformité

Remplacer le texte existant de l'Article 8 par le nouveau texte suivant:

8.1 Généralités

Les exigences de conformité statique spécifient les éléments qui doivent, qui peuvent et qui ne doivent pas être mis en œuvre dans le cadre d'une mise en œuvre revendiquant la conformité au présent document.

Noter que cette section ne fait référence qu'aux paramètres définis à l'Article 5. La norme de référence fournit d'autres déclarations de PICS liés à la TLS en plus de spécifier une exigence facultative.

8.2 Notation

Les notations suivantes sont utilisées pour spécifier les exigences de conformité:

o: Prise en charge obligatoire. L'élément doit être mis en œuvre.

f: Prise en charge facultative. L'élément peut être, mais n'a pas besoin d'être, mis en œuvre.

x: Exclus. L'élément ne doit pas être pris en charge.

8.3 Conformité aux suites chiffrées sélectionnées

Le Tableau 1 indique les exigences de conformité pour les suites chiffrées TLS, définies en 5.1.