IEC 62351-3

Edition 1.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données –
Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP

IEC 62351-3:2014-10/AMD1:2018-05(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

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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions 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.

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.

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.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

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 aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions 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.

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.

IEC 62351-3

Edition 1.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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 978-2-8322-5720-3

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

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

FDIS	Report on voting
57/1976/FDIS	57/1990/RVD

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

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 amendment and the base publication will remain unchanged until the stability date indicated on the IEC website 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.

---

2 Normative references

Replace the existing reference IEC TS 62351-9 with the following new reference:

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

Replace the existing reference IEC/ISO 9594-8 with the following new reference:

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

4.1 Operational requirements affecting the use of TLS in the telecontrol environment

Replace the existing text of the fifth paragraph of 4.1 with the following new text:

Note that TLS utilizes X.509 certificates (see also ISO/IEC 9594-8 or RFC 5280) for authentication. In the context of this specification the term certificates always relates to public-key certificates (in contrast to attribute certificates).

4.2 Security threats countered

Replace the existing text of the second paragraph of 4.2 with the following new text:

TCP/IP and the security specifications in this part of IEC 62351 cover only to the communication transport layers (OSI layers 4 and lower). 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.

NOTE The application of TLS as profiled in this document supports the protection of information sent over the TLS protected connection.

4.3 Attack methods countered

Replace the existing text of the first bullet point of Subclause 4.3 by the following new text:

– Man-in-the-middle: This threat is countered through the use of a Message Authentication Code mechanism or digital signatures specified within this document.

5.1 Deprecation of cipher suites

Add the following new text before the fourth paragraph of 5.1:

The support of SHA-1 is intended for backward compatibility. SHA-256 shall be supported and is the preferred signature algorithm to be used.

SHA-1 is no longer recognized as secure with respect collision resistance and it is therefore strongly recommended to perform a risk assessment before using this algorithm. If SHA-256 cannot be used, it is also recommended that additional security measures be taken. The usage of SHA-1 will be disallowed in the next edition of this standard.

NOTE Recommendations regarding hash signature algorithms are reviewed constantly and can be found in NIST SP800-57, BNetzA (BSI), or the NSA Suite B.

Replace the existing text of the fourth paragraph of 5.1 by the following new text:

The list of disallowed suites includes, but is not limited to:

– TLS_NULL_WITH_NULL_NULL
– TLS_RSA_ WITH_NULL_MD5

5.2 Negotiation of Versions

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

The proposal of versions TLS 1.0 or TLS 1.1 should raise a security warning ("warning: insecure TLS version"). Implementations should provide a mechanism for announcing security warnings.

5.3 Session Resumption

Replace the existing text of Subclause 5.3 with the following new text:

Session resumption in TLS allows for the resumption of a session based on the session ID connected with a dedicated (existing) master secret, which will result in a new session key. This minimizes the performance impact of asymmetric handshakes, and can be done during a running session or after a session has ended within a defined time period (TLS suggests not more than 24 hours in RFC 5280). This specification follows this suggestion. Session resumption should be performed at least every 24 hours for active sessions or not later than 24 hours for sessions that have ended. The actual parameters should be defined based on

risk assessment from the referencing standard. Session resumption is expected to be more frequent than session renegotiation.

Implementations claiming conformance to this standard shall specify that the symmetric session keys shall be renewed within the maximum time period. This resumption maximum time constraint is expected to be specified in a PIXIT of the referencing standard. The maximum time period for session resumption shall be aligned with the CRL refresh time.

Session resumption intervals shall be configurable, so long as they are within the specified maximum time period.

Clients shall initiate session resumption using the *ClientHello* message. A server initiated update of session parameter shall use the *HelloRequest* message to trigger the client to send a *ClientHello* message on the currently active connection.

NOTE According to RFC 5246 the *HelloRequest* is an optional message that the server may send to a client.

Session resumption may be initiated by either side, as long as the security policies for both the client and the server permit this. In case of failures to resume a session, the failure handling described in TLS v1.2 shall be followed.

Session resumption may be done based on the session identifier (native TLS according to RFC 5246). Alternatively, session resumption may be done based on session tickets (RFC 5077). The latter option allows for avoiding server-side state for sessions, which can be resumed. This option may apply for constraint devices to avoid a larger session cache.

NOTE Application of session tickets to avoid the session specific storage on the server side provides the benefit in environments that tear down a connection and reconnect after a specific time. If session resumption is used to update the session key of an ongoing session, there may be no benefit.

The session resumption approach may be specified by the referencing standard.

5.4 Session renegotiation

Replace the existing text of the second and the third paragraphs of 5.4 with the following new text:

Session renegotiation intervals shall be configurable so long as they are within the specified maximum time period, and shall be aligned with the CRL update period. If the Online Certificate Status Protocol (OCSP) is used for certificate revocation checks, session renegotiation shall be aligned with the OCSP response cache time. In any case, for long lasting connections renegotiation shall be performed at least every 24 hours to enforce the certificate validity check. Shorter intervals may be defined by the referencing standard.

NOTE An example alignment is ½ CRL refresh time or ½ OCSP response caching time to limit the possibility of undetected revoked certificates.

Implementations claiming conformance to this standard shall specify that the master secret shall be renegotiated within a maximum time period. This renegotiation maximum time constraint is expected to be specified in a PIXIT (Protocol Implementation eXtra Information for Testing) of the referencing standard.

Replace the existing text of the fourth paragraph of 5.4 with the following new text:

TLS Clients shall initiate session renegotiation using the *ClientHello* message. A TLS server initiated update of session parameter shall use the *HelloRequest* message to trigger the TLS client to send a *ClientHello* message on the currently active connection.

NOTE According to RFC 5246 the *HelloRequest* is an optional message that the server may sent to a client.

Session renegotiation may be initiated by either side, so long as both the TLS client and TLS server are allowed to use this feature by their security policy. In case of failures to renegotiate a session, the failure handling described in TLS v1.2 shall be followed.

The calling entity is 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 from the called entity at the expected interval, then the calling entity shall terminate the connection. The termination of a connection due to a missed session renegotiation should raise a security event ("incident: session renegotiation interval expired"). Implementations should provide a mechanism for announcing security events.

NOTE It is expected that client and server are configured with the same TLS security policy.

5.5 Message Authentication Code

Add the following new text at the end of 5.5:

The specific algorithm is indicated by the cipher suite.

5.6.1 Multiple Certification Authorities (CAs)

Replace the existing first paragraph of 5.6.1 with the following new text:

An implementation claiming conformance to this standard shall support more than one Certification Authority related trust anchor. The actual number is expected to be declared in the implementation's PIXIT statement.

5.6.3 Certificate exchange

Replace the existing text of Subclause 5.6.3 with the following new text:

The certificate exchange and validation shall be bi-directional to achieve mutual authentication. If either entity does not provide its certificate, the connection shall be terminated.

NOTE 1 The server certificate is conveyed in the *ServerHello* message. The client certificate is conveyed in the *Certificate* message.

The connection termination due to the lack of a certificate of either side should raise a security event ("incident: certificate unavailable"). Implementations should provide a mechanism for announcing security events.

NOTE 2 The option to remotely monitor security events is preferred.

5.6.4.4 Certificate revocation

Replace the existing text of Subclause 5.6.4.4 with the following new text:

Certificate revocation shall follow the mandatory parameters and procedures specified in ISO/IEC 9594-8.

The management of the Certificate Revocation List (CRL) is a local implementation issue. Discussion of the management issues regarding CRLs can be found in IEC TS 62351-1. Alternatively to local CRLs, OCSP may be used to check the revocation state of applied certificates. The application of OCSP is outlined in IEC 62351-9.

An implementation claiming conformance to this standard shall be capable of checking the local CRL at a configurable interval. The process of checking the CRL shall not cause an established session to be terminated. An inability to access the CRL shall not cause the session to be terminated.

Revoked certificates shall not be used in the establishment or renegotiation of a TLS session. An entity receiving a revoked certificate during session establishment shall refuse the connection. An entity receiving a revoked certificate during session renegotiation shall terminate the connection.

Other standards referencing this standard shall specify recommended default evaluation intervals. The referencing standard shall determine the action that shall be taken if a certificate, currently in use, has been revoked.

Note that through the normal application/distribution of CRL(s), connections may be terminated, thus creating an inability to perform communications. Therefore system administrators should develop certificate management procedures to mitigate such an occurrence (see also IEC 62351-9). Also, it is expected that there is a security management process in place to evaluate the CRL before distribution to avoid an invalid teardown of the communication connection, which may influence the reliability. There may also be support for multiple certificates per device to switch on the fly to another (valid) certificate.

The refusal / termination of a connection due to a revoked certificate should raise a security event ("incident: revoked certificate"). Implementations should provide a mechanism for announcing security events.

NOTE The option to remotely monitor security events is preferred.

5.6.4.5 Expired certificates

Replace the existing text of Subclause 5.6.4.5 with the following new text:

Expired certificates shall not be used in the establishment or renegotiation of a TLS session. An entity receiving an expired certificate during session establishment shall refuse the connection. An entity receiving an expired certificate during session renegotiation shall terminate the connection.

Note that it is expected that there is a security management process in place to initiate a timely certificate renewal procedure (see also IEC 62351-9). An example time frame may be a month. There may also be support for multiple certificates per device to permit the switch to another (valid) certificate.

The refusal of a connection due to an expired certificate should raise a security event ("warning: expired certificate"). Implementations should provide a mechanism for announcing security events.

NOTE The option to remotely monitor security events is preferred.

5.6.4.6 Signing

Add the following new text before the first NOTE in 5.6.4.6:

Security policies of entities shall be able to disallow or prevent any optional key length being supported.

Add the following new text at the end of 5.6.4.6:

Optional support for ECDSA using the curve brainpoolP256r1 may be supported. The OID for this curve is: iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7).

The support of SHA-1 is intended for backward compatibility. SHA-256 shall be supported and is the preferred signature algorithm to be used.

SHA-1 is no longer recognized as secure with respect collision resistance and it is therefore strongly recommended to perform a risk assessment before using this algorithm. If SHA-256 cannot be used, it is also recommended that additional security measures be taken. The usage of SHA-1 will be deprecated in the next edition of this standard.

Security policies of entities shall be able to disallow or prevent any optional hashing algorithms being supported.

NOTE Recommendations regarding hash signature algorithms are reviewed constantly and can be found in NIST SP800-57, BNetzA (BSI), or the NSA Suite B.

5.6.4.7 Key exchange

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

Public key mechanisms (based on RSA) as well as Diffie-Hellman and ephemeral Diffie-Hellman mechanisms shall be supported. For the key exchange algorithms, the following key length shall be supported:

– Optional: Minimum RSA key length of 1024 Bit (legacy mode);
– Mandatory: Recommended RSA key length of at least 2048 Bit (modern mode).

The optional support for 1024 bit RSA key length is intended for backward compatibility. 2048 bit key length shall be supported and is the preferred key length to be used. The application of RSA keys with 1024 Bit should raise a security warning ("warning: minimum key length"). Implementations should provide a mechanism for announcing security warnings.

A 1024 bit RSA key length for the key exchange is no longer recognized as secure and it is therefore strongly recommended to perform a risk assessment before using these keys. If a longer key length than 1024 bits cannot be used, it is also recommended to take additional security measures. The usage of 1024 bit key length will be deprecated in the next edition of this standard. IEC 62351-9 provides further information on the life cycles of cipher strengths.

Security policies of entities shall be able to disallow or prevent any optional key length being supported..If any of the public key mechanisms based on elliptic curves are supported (e.g., ECDSA) as well as elliptic curve based Diffie-Hellman and ephemeral elliptic curve based Diffie-Hellman mechanisms are supported, the following key length shall be supported:

Mandatory: Minimum ECDSA key length of 256 Bit

NOTE There are cipher suites defined for TLS supporting also a mixture of both RSA based signatures and elliptic curve based Diffie Hellman.

TLS clients using TLS version 1.2 shall include the `signature_algorithm` extension with at least the combination of `{RSA, SHA-1; RSA, SHA-256; ECDSA, SHA256}` in the client hello message. Other combinations may be supported.

NOTE If the `signature_algorithm` is not included, TLS 1.2 server will fall back to default, which is SHA-1.

The support of SHA-1 is intended for backward compatibility. SHA-256 shall be supported and is the preferred signature algorithm to be used.

SHA-1 is no longer recognized as secure with respect collision resistance and it is therefore strongly recommended to perform a risk assessment before using this algorithm. If SHA-256 cannot be used, it is also recommended that additional security measures be taken. The usage of SHA-1 will be deprecated in the next edition of this standard.

Security policies of entities shall be able to disallow or prevent any optional hashing algorithms being supported.

NOTE Recommendations regarding hash signature algorithms are reviewed constantly and can be found in NIST SP800-57, BNetzA (BSI), or the NSA Suite B.

7 Referencing Standard Requirements

Replace the existing text of Clause 7 with the following new text:

Other standards referencing this standard shall specify:

– The mandatory TLS cipher suites to be supported.

– The recommended specification in regards to session resumption method and parameters from a previous connection based upon session run-time. Note this time shall not be larger than 24 hours.

– The recommended specification in regards to the renegotiation of session parameters based upon session run-time. Session renegotiation should always be aligned with the CRL refresh time to avoid unnecessary certificate revocation checks.

– Individual certificate fields, if the certificate validation shall be restricted to only dedicated certificates from an authorized CA (instead of allowing all certificates).

– The recommended number of CAs to be supported.

– The TCP port to be used in order to differentiate between secure (e.g. using TLS) and non-secure communication traffic.

– The maximum public key certificate size.

– The recommended default certificate revocation evaluation period.

– If OCSP is used for certificate revocation checks, the handling of failures to access the OCSP responder.

– The handling of certificate validation actions with respect to certificates used in the context of TLS, since the revocation or expiration of a certificate influences the security of the connection. Appropriate measures shall be specified to ensure service and system availability.

– The handling of security events defined in this part.

– The required conformance to this standard.