

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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 It also gives information on projects, replaced and withdrawn publications.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 between 2002 and 2015. 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 entre 2002 et 2015. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.



IEC 62351-3

Edition 1.2 2020-02
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Power systems management and associated information exchange – Data
and communications security –**

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

**Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –**

**Partie 3: Sécurité des réseaux et des systèmes de communication – Profils
comprenant TCP/IP**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-7772-0

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.

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

REDLINE VERSION

VERSION REDLINE



**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**

CONTENTS

FOREWORD	3
INTRODUCTION to Amendment 2	5
1 Scope	6
1.1 Scope	6
1.2 Intended Audience	6
2 Normative references	6
3 Terms, definitions and abbreviations	7
3.1 Terms, definitions and abbreviations	7
3.2 Additional abbreviations	7
4 Security issues addressed by this standard	7
4.1 Operational requirements affecting the use of TLS in the telecontrol environment	7
4.2 Security threats countered	8
4.3 Attack methods countered	8
4.4 Handling of security events	8
5 Mandatory requirements	9
5.1 Deprecation of cipher suites	9
5.2 Negotiation of versions	9
5.3 Session resumption	10
5.4 Session renegotiation	11
5.5 Message Authentication Code	12
5.6 Certificate support	12
5.7 Co-existence with non-secure protocol traffic	16
6 Optional security measure support	16
7 Referencing standard requirements	17
8 Conformance	17
8.1 General	17
8.2 Notation	17
8.3 Conformance to selected cipher suites	18
8.4 Conformance to selected TLS versions	18
8.5 Conformance to selected TLS protocol features	18
8.6 Conformance to certificate support	19
8.7 Conformance to cryptographic algorithm support	19
Bibliography	20
Table 1 – Conformance to TLS cipher suites	18
Table 2 – Conformance to TLS versions	18
Table 3 – Conformance to TLS protocol features	18
Table 4 – Conformance to certificate support	19
Table 5 – Conformance to cryptographic algorithm support	19

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendments has been prepared for user convenience.

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

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendments 1 and 2. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION to Amendment 2

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

- Support for TLS versions 1.1 and 1.0 is made optional instead of mandatory to address known weaknesses. This is aligned with the defined security warnings for TLS versions 1.1 and 1.0.
- Update of TLS version handling during renegotiation and resumption to avoid TLS version downgrade/upgrade within a same session.
- Updated explanatory text for session renegotiation to make the communication relations clearer.
- Deprecation of RSA1024 and SHA-1 algorithms. This underlines the desire to disallow them in the next edition.
- Inclusion of PICS section for mandatory and optional settings in TLS.
- Updated text for and enhancements of security events to better align with IEC 62351-14
- Inclusion of general remarks for the security event handling.
- Update of references.

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

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

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

1 Scope

1.1 Scope

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

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

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

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

1.2 Intended Audience

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

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

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

2 Normative references

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

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

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

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

IEC ~~TS~~ 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*⁴

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

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

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

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

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

RFC 6066:2006, *Transport Layer Security Extensions*

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

3 Terms, definitions and abbreviations

3.1 Terms, definitions and abbreviations

For the purposes of this document, the terms, definitions and abbreviations given in IEC TS 62351-2, Glossary, apply.

3.2 Additional abbreviations

CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
ECDSA	Elliptic Curve Digital Signature Algorithm
ECGDSA	Elliptic Curve German Digital Signature Algorithm (see ISO/IEC 15946-2)
OCSP	Online Certificate Status Protocol (see RFC 6960)
PIXIT	Protocol Implementation eXtra Information for Testing

4 Security issues addressed by this standard

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

The IEC telecontrol environment has different operational requirements from many Information Technology (IT) applications that make use of TLS in order to provide security protection. The most differentiating, in terms of security, is the duration of the TCP/IP connection for which security needs to be maintained.

Many IT protocols have short duration connections, which allow the encryption algorithms to be renegotiated at connection re-establishment. However, the connections within a telecontrol environment tend to have longer durations, often “permanent”. It is the longevity of the connections in the field of power systems management and associated information exchange that give rise to the need for special consideration. In this regard, in order to provide protection for the “permanent” connections, a mechanism for updating the session key is specified within this standard, based upon the TLS features of session resumption and

⁴ ~~Under consideration.~~

² This is typically referred to as SSL/TLS.

session re-negotiation while also considering the relationship with certificate revocation state information.

Another issue addressed within this standard is how to achieve interoperability between different implementations. TLS allows for a wide variety of cipher suites to be supported and negotiated at connection establishment. However, it is conceivable that two implementations could support mutually exclusive sets of cipher suites. This standard specifies that referring standards must specify at least one common cipher suite and a set of TLS parameters that allow interoperability.

Additionally, this standard specifies the use of particular TLS capabilities that allow for specific security threats to be countered.

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).

NOTE It is intended that certificate management necessary to operate TLS be specified in compliance with IEC TS 62351-9.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

TCP/IP and the security specifications in this part of IEC 62351 cover only ~~to~~ 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.

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

The specific threats countered in this part of IEC 62351 for the transport layers include:

- Unauthorized modification or insertion of messages through message level authentication and integrity protection of messages.

Additionally, when the information has been identified as requiring confidentiality protection:

- Unauthorized access or theft of information through message level encryption of the messages

4.3 Attack methods countered

The following security attack methods are countered through the appropriate implementation of the specifications and recommendations in this part of IEC 62351.

- Man-in-the-middle: This threat is countered through the use of a Message Authentication Code mechanism or digital signatures specified within this document.
- Replay: This threat is countered through the use of specialized processing state machines specified by the normative references of this document.
- Eavesdropping: This threat is countered through the use of encryption.

NOTE The actual performance characteristics of an implementation claiming conformance to this standard are out-of-scope of this standard.

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

Any cipher suite that specifies NULL for encryption shall not be used for communication outside the administrative domain, if the encryption of this communication connection by other means cannot be guaranteed.

NOTE 1 This standard does not exclude the use of encrypted communications through the use of cryptographic based VPN tunnels. The use of such VPNs is out-of-scope of this standard.

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

- ~~— TLS_RSA_NULL_WITH_NULL_SHA~~
- ~~— TLS_RSA_NULL_WITH_NULL_SHA256~~
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256

NOTE 2 The application of no-encryptng cipher suites allows for traffic inspection while still retaining an end-to-end authentication and integrity protection of the traffic.

Implementations allowing TLS cipher suites with NULL encryption claiming conformance to this part shall provide a mechanism to explicitly enable those TLS cipher suites. Per default, non-encrypting TLS cipher suites are not allowed.

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.

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.

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

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_~~NULL~~_WITH_NULL_MD5

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

TLS v1.2 as defined in RFC 5246 (sometimes referred to as SSL v3.3) ~~or higher~~ 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 ~~shall also~~ 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 ~~IEC 62351~~ 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.

The proposal of versions prior to TLS 1.0 or SSL 3.1 ~~should~~ shall raise a security event ("incident: ~~unsecure communication~~") ("alarm: unsecure communication"). ~~Implementations should provide a mechanism for announcing security events.~~

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").

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

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 5246). This specification follows this ~~approach~~ suggestion. Session resumption should be performed ~~in less~~ at least every 24 hours for active sessions or not later than 24 hours for sessions that have ended, ~~but~~. 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 leading to a smaller session resumption interval than the session renegotiation interval. ($0 < \text{session resumption interval} < \text{session renegotiation interval} \leq 24\text{h}$).

Implementations claiming conformance to this standard shall specify that the symmetric session keys ~~to~~ shall be renewed within the maximum time period ~~and maximum allowed number of packets/bytes sent. These~~ This resumption maximum time/bytes constraints are constraint is expected to be specified in a ~~PIXT~~ PICS 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, ~~so~~ as long as the security policies for both the client and the server, ~~are allowed to use this feature by their security policy~~ 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.

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

5.4 Session renegotiation

Session renegotiation in TLS requires a complete TLS handshake where all asymmetric operations and certificate checks must be performed. Session renegotiation will result in a completely new session based upon both a freshly negotiated master key and a new session key. During the TLS handshake phase, the certificates are also checked for their validity and their revocation state. Hence, the timeframe for session renegotiation should be chosen in accordance to the refresh of the revocation state information (CRL) as described in 5.6.4.4.

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, ~~instead of using CRLs~~, 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 ~~for long lasting connections~~ to enforce the certificate validity check. Shorter intervals may be defined by the referencing standard.

NOTE An example alignment is $\frac{1}{2}$ CRL refresh time or $\frac{1}{2}$ 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 ~~and a maximum allowed number of packets/bytes sent. These~~ This renegotiation maximum time/bytes constraints ~~are~~ is expected to be specified in a ~~PIKIT (Protocol Implementation eXtra Information for Testing)~~ PICS of the referencing standard.

~~The initiation of the TLS (renegotiation) handshake sequence shall be the responsibility of the TCP entity that receives the TCP_OPEN indication (e.g. the called entity). A request to change the cipher, issued from the calling entity (e.g. the node that issued the TCP_OPEN) shall be ignored.~~

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 (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").

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

There shall be a timeout associated with the response to a change cipher request. A timeout of the change cipher request shall result in the connection being terminated. The timeout value shall be configurable.

To avoid weaknesses in session renegotiation, the session renegotiation extension defined in RFC 5746 shall be used.

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.

5.5 Message Authentication Code

The Message Authentication Code shall be used. TLS has this capability specified as an option. This standard mandates the use of this capability to aid in countering and detecting man-in-the-middle attacks. The specific algorithm is indicated by the cipher suite.

5.6 Certificate support

5.6.1 Multiple Certification Authorities (CAs)

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

The criteria and selection of a CA is out-of-scope of this standard.

In scenarios where more than one X.509 certificate (and corresponding private key) is available on an IED, it may be desirable to enable the requester to choose a certificate on the IED side that matches the trusted anchor (root CA) certificates available at the requester side.

The Trusted CA Indication extension specified in RFC 6066 allows a TLS client to provide information about locally supported CA certificates since the root CA of the utilities may not be public. The extension allows the requesting party to influence the selection of the X.509 certificate on the IED side for the server side authentication to enable the verification of the used X.509 certificate on the requestor side.

The Trusted CA Indication is contained in the client hello message. A TLS server receiving a Trusted CA Indication may use this information to guide its selection of an appropriate certificate chain to return to the client. According to RFC 6066 in this event, the server shall include an extension of type "trusted_ca_keys" in the (extended) server hello. The "extension_data" field of this extension shall be empty.

The support of this extension may be applicable in scenarios where IEDs are accessed by different administrative domains, e.g., two utilities with an own public key infrastructure. If different administrative domains are to be supported, the TLS Trusted CA Indication extension shall be used.

Implementations claiming conformance to this standard using this extension shall specify the selection of the requested CA issued certificates on the TLS server side. This needs to be specified for the success and failure case of a matching CA issued certificate. It is a PIXIT issue, of the referencing standard, to specify the constraints on the Trusted CA Indication handling.

The failure of selecting a matching CA issued certificate ~~should~~ shall raise a security event ("incident: CA not found") ("alarm: CA certificate not found"). ~~Implementations should provide a mechanism for announcing security events.~~

NOTE The option to remotely monitor security events is preferred.

5.6.2 Certificate size

A protocol specifying the use of this standard shall specify the maximum size of certificate allowed to be used. It is recommended that this size shall be less than or equal to 8 192 octets.

NOTE 1 The certificate may also carry role information according to IEC TS 62351-8, which influences its final size.

NOTE 2 The certificate size may be influenced by the careful selection of names in issuer and subject field and supported extensions, etc.

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

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~~ shall raise a security event ~~("incident: certificate unavailable")~~ ("alarm: 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 Public-key certificate validation

5.6.4.1 General

Certificates shall be validated by both the calling and called nodes. There are two mechanisms that shall be configurable for certificate verification.

- Acceptance of any certificate from an authorized CA
- Acceptance of individual certificates from an authorized CA

5.6.4.2 Verification based upon CA

An implementation claiming conformance to this standard shall be capable of being configured to accept certificates from one or more Certificate Authorities without the configuration of individual certificates.

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

An implementation claiming conformance to this standard shall be capable of being configured to accept specific individual certificates from one or more authorized Certificate Authorities (e.g. configured).

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

Certificate revocation shall ~~be performed as~~ 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 ~~TS~~ 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.

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")."

~~The revocation of a certificate shall terminate any session established using that certificate.~~

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~~ shall raise a security event ~~("incident: revoked certificate")~~ ("alarm: revoked certificate"). ~~Implementations should provide a mechanism for announcing security events.~~

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

5.6.4.5 Expired certificates

~~The expiration of a certificate shall not cause connections to be terminated.~~

~~An expired certificate shall not be used or accepted during connection establishment or a session renegotiation.~~

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~~ shall raise a security event ~~("warning: expired certificate")~~ ("alarm: expired certificate"). ~~Implementations should provide a mechanism for announcing security events.~~

NOTE The option to remotely monitoring security events is preferred.

5.6.4.6 Signing

Signing through the use of RSA or DSS algorithms shall be supported. Other algorithms, e.g., those based on elliptic curve cryptography like ECDSA or ECGDSA may be specified in standards that reference this document.

For RSA-based signatures, the following key length shall be supported:

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

- Mandatory: Signature-operation: RSA with a key length of at least 2 048 Bits ~~(modern mode).~~

~~The optional support of RSA with 1 024 bit keys is intended for backward compatibility and affects mainly the receiver side. RSA with 2 048 bit keys must be supported and is the preferred signature algorithm to be used.~~

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.

1 024 bits RSA is no longer recognized as secure with respect to the key length and it is therefore strongly recommended to perform a risk assessment before using these keys. If longer keys than 1 024 bits cannot be used, it is also recommended that additional security measures be taken. The usage of 1 024 bit RSA will be deprecated in the next edition of this standard. IEC/TS 62351-9 will provide 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.

NOTE Recommendations regarding required key length for signature algorithms are reviewed constantly and can be found in NIST SP800-57, BnetZA (BSI), or the NSA Suite B.

Optional Signature-operation: Elliptic curves defined over finite prime fields with signature algorithm ECDSA or ECGDSA (for ECGDSA, see ISO/IEC 15946-2). The recommended minimum key length is 256 bits (in combination with SHA-256). The OID to for ecdsa-with-SHA256 to be used is: iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2. Cipher suites for TLS, which utilize ECDSA are defined in RFC 4492 as well as in RFC 5246.

The curve to be used for ECDSA shall be secp256r1. The OID for this curve is: iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7.

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 deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash 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.

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

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 must 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.~~

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").

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 ~~TS~~ 62351-9 ~~will~~ 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 deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash 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.

5.7 Co-existence with non-secure protocol traffic

Referencing standards shall provide a separate TCP/IP port through which to exchange TLS secured traffic. This will allow for the possibility of un-ambiguous secure and non-secure communications simultaneously.

6 Optional security measure support

In certain deployments, additional support is necessary to further restrict the usage of certificates based on their serial numbers and issuers. This restriction is known as certificate white listing or certificate pinning, and is currently being defined in the IETF. Certificate white listing can be optionally supported. If an implementation supports certificate white listing, a white list shall be built by stating the serial number and the issuer of the allowed certificates. As this approach is not restricted to the usage of certificates in TLS, it is further specified in IEC TS 62351-9.

7 Referencing standard requirements

Other standards referencing this standard shall specify:

- The mandatory TLS cipher suites to be supported.
- If other versions than TLS 1.2 are to be used, the referencing standard shall define the required versions.
- ~~– The recommended time period in which encryption keys are to be exchanged (session key update).~~
- The recommended specification in regards to session resumption ~~of keys~~ method and parameters from a previous connection based upon ~~protocol traffic and/or session run-time. This shall specify the mechanism to measure the traffic (e.g. packets sent, bytes sent, etc.) and the recommended metric upon which session resumption should be performed.~~ Note this time shall not be larger than 24 hours.
- The recommended specification in regards to the renegotiation of ~~keys~~ session parameters based upon ~~protocol traffic and/or session run-time. This shall specify the mechanism to measure the traffic (e.g. packets sent, bytes sent, etc.) and the recommended metric upon which session renegotiation should be performed.~~ 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 ~~CRL~~ certificate revocation evaluation period.
- ~~In case of using~~ If OCSP is used for certificate revocation checks, the handling of failures to access the OCSP responder.
- The handling of certificate ~~revocation~~ validation actions with respect to certificates used in the context of TLS. ~~Revoking~~, 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.

8 Conformance

~~Conformance to this part of IEC 62351 shall be determined by the implementation of all parts of Clause 5.~~

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		

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

ISO/IEC 15946-2, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures* (withdrawn)

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

IEC TS 62351-8:2011, *Power systems management and associated information exchange Data and communications security – Part 8: Role-based access control*

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Events Logs*³

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

NIST SP-800-57 Part 1 Rev. 3, *Recommendations for Key Management*, July 2012

BNetzA, BSI, *Algorithms for Qualified Electronic Signatures*, 02/2013.

NSA Suite B, *Suite B Cryptography / Cryptographic Interoperability*

³ Under preparation. Stage at the time of publication: IEC/PCC 62351-14:2020.

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

SOMMAIRE

AVANT-PROPOS	23
INTRODUCTION à l'Amendement 2	25
1 Domaine d'application	26
1.1 Domaine d'application	26
1.2 Utilisateurs prévus	26
2 Références normatives	27
3 Termes, définitions et abréviations	27
3.1 Termes, définitions et abréviations	27
3.2 Autres abréviations	28
4 Problèmes de sécurité couverts par la présente norme	28
4.1 Influence des exigences fonctionnelles sur l'utilisation de la TLS dans l'environnement de téléconduite	28
4.2 Menaces à la sécurité contrées	28
4.3 Méthodes d'attaques contrées	29
4.4 Gestion des événements de sécurité	29
5 Exigences obligatoires	30
5.1 Rejet de suites chiffrées	30
5.2 Négociation des versions	30
5.3 Reprise de session	31
5.4 Renégociation de session	32
5.5 Code d'authentification de message	33
5.6 Prise en charge du certificat	34
5.7 Coexistence avec un trafic de protocole non sécurisé	39
6 Prise en charge de mesures de sécurité – facultatif	40
7 Exigences relatives aux normes de référence	40
8 Conformité	40
8.1 Généralités	41
8.2 Notation	41
8.3 Conformité aux suites chiffrées sélectionnées	41
8.4 Conformité aux versions TLS sélectionnées	41
8.5 Conformité aux caractéristiques de protocole TLS sélectionnées	42
8.6 Conformité à la prise en charge des certificats	42
8.7 Conformité à la prise en charge des algorithmes cryptographiques	42
Bibliographie	44
Tableau 1 – Conformité aux suites chiffrées TLS	41
Tableau 2 – Conformité aux versions TLS	41
Tableau 3 – Conformité aux caractéristiques de protocole TLS	42
Tableau 4 – Conformité à la prise en charge des certificats	42
Tableau 5 – Conformité à la prise en charge des algorithmes cryptographiques	43

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

Cette version consolidée de la Norme IEC officielle et de ses amendements a été préparée pour la commodité de l'utilisateur.

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

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par les amendements 1 et 2. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

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

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de ses amendements ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION à l'Amendement 2

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

- Prise en charge des versions TLS 1.1 et 1.0 rendue facultative plutôt qu'obligatoire pour remédier aux faiblesses connues. Cette possibilité permet de s'aligner sur les avertissements de sécurité définis pour les versions TLS 1.1 et 1.0.
- Mise à jour de la gestion des versions TLS lors de la renégociation et de la reprise pour éviter une mise à niveau inférieur/supérieur des versions TLS au cours d'une même session.
- Mise à jour du texte explicatif de la renégociation de session pour clarifier davantage les relations de communication.
- Rejet des algorithmes RSA1024 et SHA-1. Cette démarche souligne la volonté de les interdire dans la prochaine édition.
- Inclusion de la section des PICS pour les paramètres obligatoires et facultatifs dans la TLS.
- Mise à jour du texte et améliorations des événements de sécurité pour mieux s'aligner sur l'IEC 62351-14.
- Inclusion de remarques générales sur la gestion des événements de sécurité.
- Mise à jour des références.

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

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP

1 Domaine d'application

1.1 Domaine d'application

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

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

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

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

1.2 Utilisateurs prévus

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

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

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

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

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

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

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

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

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

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

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

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

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

3 Termes, définitions et abréviations

3.1 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviations de l'IEC TS 62351-2, Glossaire, s'appliquent.

¹ ~~A l'étude.~~

² Généralement appelé SSL/TLS.

3.2 Autres abréviations

CRL	Liste de révocation de certificat (<i>Certificate Revocation List</i>)
DER	Règles de codage identifiées (<i>Distinguished Encoding Rules</i>)
ECDSA	Algorithme de signature numérique de courbe elliptique (<i>Elliptic Curve Digital Signature Algorithm</i>)
ECGDSA	Algorithme de signature numérique allemand de courbe elliptique (<i>Elliptic Curve German Digital Signature Algorithm</i>) (voir l'ISO/IEC 15946-2)
OCSF	Protocole de vérification en ligne de certificat (<i>Online Certificate Status Protocol</i>) (voir la RFC 6960)
PIXIT	Informations complémentaires de mise en œuvre du protocole pour les essais (<i>Protocol Implementation eXtra Information for Testing</i>)

4 Problèmes de sécurité couverts par la présente norme

4.1 Influence des exigences fonctionnelles sur l'utilisation de la TLS dans l'environnement de téléconduite

L'environnement de téléconduite de l'IEC comporte différentes exigences fonctionnelles correspondant à plusieurs applications de technologie de l'information (IT, *Information Technology*) qui utilisent la TLS pour assurer une protection en matière de sécurité. En termes de sécurité, la durée de la connexion TCP/IP pour laquelle il est nécessaire de maintenir la sécurité est le critère le plus déterminant.

De nombreux protocoles IT ont des durées de connexion courtes qui permettent la renégociation des algorithmes de chiffrement lors du rétablissement de la connexion. Cependant, les connexions dans un environnement de téléconduite ont tendance à être plus longues, et sont souvent "permanentes". En raison de leur longévité, les connexions dans le domaine de la gestion des systèmes de puissance et échanges d'informations associés nécessitent une prise en compte particulière. À cet effet, afin d'assurer la protection des connexions "permanentes", un mécanisme de mise à jour de la clé de session est spécifié dans la présente norme, sur la base des caractéristiques TLS de reprise et de renégociation de session, tout en tenant également compte de la relation avec les informations d'état de révocation de certificat.

La présente norme couvre également le problème de l'interopérabilité entre les différentes mises en œuvre. La TLS permet de prendre en charge et de négocier une grande variété de suites chiffrées lors de l'établissement de la connexion. Cependant, il est imaginable que deux mises en œuvre puissent prendre en charge des ensembles mutuellement exclusifs de suites chiffrées. La présente norme spécifie que les normes de référence doivent indiquer au moins une suite chiffrée commune et un ensemble de paramètres TLS autorisant l'interopérabilité.

De plus, la présente norme spécifie l'utilisation de capacités TLS particulières qui permettent de contrer des menaces spécifiques pesant sur la sécurité.

Noter que la TLS utilise des certificats X.509 (voir aussi l'ISO/IEC 9594-8 ou la RFC 5280) pour l'authentification. Dans le contexte de la présente spécification, le terme certificat fait toujours référence à des certificats de clé publique (par opposition aux certificats d'attribut).

NOTE Il est prévu qu'une gestion des certificats nécessaire pour faire fonctionner la TLS soit spécifiée conformément à l'IEC TS 62351-9.

4.2 Menaces à la sécurité contrées

Voir l'IEC TS 62351-1 pour des informations sur les menaces à la sécurité et les méthodes d'attaque.

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 ~~pour les~~ spécifique aux couches application de communication (couches OSI 5 et supérieures) ou la sécurité d'application à application.

NOTE L'application de TLS décrite dans le présent document prend en charge la protection des informations envoyées à la connexion TLS protégée.

Les menaces spécifiques contrées dans la présente partie de l'IEC 62351 pour les couches transport comprennent:

- la modification non autorisée ou l'insertion de messages par l'authentification des niveaux des messages et la protection de l'intégrité des messages.

De plus, lorsque les informations ont été identifiées comme exigeant une protection de la confidentialité:

- l'accès non autorisé aux informations ou le vol d'informations par le chiffrement des niveaux des messages.

4.3 Méthodes d'attaques contrées

Les méthodes suivantes d'attaque de sécurité sont contrées grâce à la mise en œuvre appropriée de spécifications et de recommandations dans la présente partie de l'IEC 62351.

- Attaque «Man-in-the-middle» (homme au milieu): Cette menace est contrée grâce à l'utilisation d'un mécanisme de code d'authentification de message ou de signatures numériques spécifiés dans le présent document.
- Attaque par rejeu: Cette menace est contrée grâce à l'utilisation de diagrammes d'états de traitement spécialisés et spécifiés dans les références normatives du présent document.
- Attaque par écoute illicite («Eavesdropping»): Cette menace est contrée grâce à l'utilisation de chiffrement.

NOTE Les caractéristiques actuelles de performance d'une mise en œuvre revendiquant la conformité à la présente norme ne relèvent pas du domaine d'application de la présente norme.

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

Une suite chiffrée qui spécifie NULL en chiffrement ne doit pas être utilisée pour la communication à l'extérieur du domaine administratif, si le chiffrement de cette connexion de communication par d'autres moyens ne peut pas être garanti.

NOTE 1 La présente norme n'exclut pas l'utilisation de connexions chiffrées à l'aide d'un tunnel VPN basé sur une cryptographie. L'utilisation de tels VPN est en dehors du domaine de l'application de la présente norme.

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

- ~~— TLS_RSA_NULL_WITH_NULL_SHA~~
- ~~— TLS_RSA_NULL_WITH_NULL_SHA256~~
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256

NOTE 2 L'application de suites chiffrées non chiffrées permet le contrôle du trafic tout en continuant à maintenir une authentification entre extrémités et une protection de l'intégrité du trafic.

Les mises en œuvre permettant des suites chiffrées TLS avec un chiffrement NULL revendiquant la conformité à la présente partie doivent fournir un mécanisme pour permettre explicitement ces suites chiffrées TLS. Par défaut, les suites chiffrées TLS sans chiffrement ne sont pas autorisées.

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.

SHA-1 n'est plus reconnu comme sécurisé par rapport à la résistance à la collision et il est donc fortement recommandé d'effectuer une appréciation du risque avant d'utiliser cet algorithme. Si SHA-256 ne peut être utilisé, il est aussi recommandé de prendre des mesures de sécurité supplémentaires. L'utilisation de SHA-1 sera rejetée dans la prochaine édition de la présente norme.

NOTE Les recommandations concernant les algorithmes de hachage sécurisé sont revues constamment et peuvent être consultées dans les documents NIST SP800-57, BnetZA (BSI), ou NSA Suite B.

La liste des suites ~~déconseillées~~ rejetées comprend les suites suivantes, ~~sans toutefois s'y limiter~~ entre autres:

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_~~NULL~~_WITH_NULL_MD5

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

La TLS v1.2 telle que définie dans la RFC 5246 (parfois appelée SSL v3.3) ~~ou~~ est la version ~~supérieure~~ 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 ~~doivent aussi~~ 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 ~~IEC 62351~~ 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.

~~Il convient que la proposition de versions inférieures à TLS 1.0 ou SSL 3.1 entraîne un événement de sécurité ("incident: communication non sécurisée"). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.~~

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.

~~Il convient que la proposition de versions TLS 1.0 ou TLS 1.1 entraîne un avertissement de sécurité («avertissement: version TLS non sécurisée»). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les avertissements de sécurité.~~

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

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

La reprise de session en TLS permet la reprise d'une session sur la base de l'ID de session connecté à un secret maître («master secret») dédié (existant), ce qui génère une nouvelle clé de session. Cela réduit le plus possible l'impact sur les performances des protocoles de transfert asymétriques et cela peut être effectué lors de la réalisation d'une session ou après la fin d'une session dans une période définie (TLS propose une durée non supérieure à 24 h dans la RFC 5246). La présente spécification adopte cette ~~méthode~~ suggestion. Il convient d'effectuer une reprise de session ~~en moins de 24 heures~~ au moins toutes les 24 h pour les sessions actives, ou au plus tard dans les 24 h après la fin d'une session, ~~mais~~. Il convient de définir les paramètres actuels sur la base de l'appréciation du risque à partir de la norme de référence. ~~Les reprises de session sont censées être plus fréquentes que les renégociations de session.~~ 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. ($0 < \text{intervalle de reprise de session} < \text{intervalle de renégociation de session} \leq 24 \text{ h}$).

Les mises en œuvre revendiquant la conformité à la présente norme doivent spécifier que les clés de session symétriques doivent être renouvelées au cours d'une période maximale ~~et pour un nombre maximal autorisé de paquets/octetes envoyés. Ces~~ Cette contraintes de temps/octetes maximaux maximale de reprise ~~sont~~ est censées être spécifiées dans des ~~PIXIT~~ PICS de la norme de référence. La période maximale de reprise de session doit être cohérente avec la période de rafraîchissement de la CRL.

Les intervalles de reprise de session doivent être configurables, tant qu'ils se trouvent dans la période maximale spécifiée.

Les clients doivent initier une reprise de session par l'intermédiaire du message *ClientHello*. Une mise à jour des paramètres de session initiée par un serveur doit utiliser le message *HelloRequest* afin que le client envoie un message *ClientHello* sur la connexion active en cours.

NOTE Selon la RFC 5246, le *HelloRequest* est un message facultatif que le serveur peut envoyer à un client.

La reprise de session peut être initiée par l'un ou l'autre côté, tant que la politique de sécurité le permet pour le client et le serveur ~~sont autorisés à utiliser cette fonctionnalité dans le cadre de leur politique de sécurité.~~ En cas d'échec de reprise d'une session, la procédure de gestion des défaillances décrite dans la TLS v1.2 doit être suivie.

La reprise de session peut être effectuée en se basant sur l'identifiant de session (TLS native selon la RFC 5246). Autrement, la reprise de session peut être effectuée en se basant sur les tickets de session (RFC 5077). Cette dernière option permet d'éviter les états côté serveur des sessions, qui peuvent être reprises. Cette option peut s'appliquer aux dispositifs de contrainte afin d'éviter une plus grande mémoire cache de session.

NOTE L'application des tickets de session pour éviter le stockage spécifique de session du côté serveur apporte des avantages aux environnements qui coupent la connexion et se reconnectent après une période spécifique. Si la reprise de session sert à mettre à jour la clé de session d'une session en cours, il peut ne pas y avoir d'avantage.

L'approche de reprise de la session peut être spécifiée par la norme de référence.

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

5.4 Renégociation de session

La renégociation de session en TLS exige un protocole de transfert TLS complet dans lequel toutes les opérations asymétriques et les vérifications de certificat doivent être effectuées. La renégociation de session génère une session entièrement nouvelle sur la base d'une clé maîtresse récemment négociée et une nouvelle clé de session. Au cours de la phase du protocole de transfert TLS, la validité et l'état de révocation des certificats sont aussi vérifiés. Il convient donc de choisir la période de renégociation de session en fonction de la période de rafraîchissement des informations de l'état de révocation (CRL), comme décrit en 5.6.4.4.

Les intervalles de renégociation de session doivent être configurables tant qu'ils se trouvent dans la période maximale spécifiée et ils doivent être cohérents avec la période de mise à jour de la CRL. Si le protocole de vérification en ligne de certificat (OCSP) est utilisé pour des vérifications de révocation de certificat ~~au lieu d'utiliser des CRL~~, la renégociation de session doit être cohérente avec le temps de mémoire cache de la réponse OCSP. Dans tous les cas, la renégociation des connexions de longue durée doit être effectuée au moins toutes les 24 h ~~pour des connexions de longue durée~~ afin d'appliquer la vérification de la validité du certificat. Des intervalles plus courts peuvent être définis par la norme de référence.

NOTE Un exemple de cohérence est $\frac{1}{2}$ période de rafraîchissement de la CRL, ou $\frac{1}{2}$ temps de mémoire cache de la réponse OCSP afin de limiter la possibilité de ne pas détecter un certificat révoqué.

Les mises en œuvre revendiquant la conformité à la présente norme doivent spécifier que le secret maître («master secret») doit être renégocié au cours d'une période maximale ~~et pour~~

~~un nombre maximal autorisé de paquets/octetes envoyés. Ces~~ Cette contraintes de temps/octetes maximaux de renégociation sont est censées être spécifiées dans des ~~PIXIT (informations complémentaires de mise en œuvre du protocole pour les essais, Protocol Implementation eXtra Information for Testing)~~ PICS de la norme de référence.

~~La responsabilité de l'initiation de la séquence de protocole de transfert (renégociation) TLS doit relever de l'entité du protocole TCP qui reçoit les indications TCP_OPEN (par exemple, l'entité appelée). Une demande de modification du chiffrement, émise par l'entité appelante (par exemple, le nœud qui a émis TCP_OPEN) doit être ignorée.~~

Les clients TLS doivent initier une renégociation de session par l'intermédiaire du message *ClientHello*. Une mise à jour des paramètres de session initiée par un serveur TLS doit utiliser le message *HelloRequest* afin que le client TLS envoie un message *ClientHello* sur la connexion active en cours.

NOTE Selon la RFC 5246, le *HelloRequest* est un message facultatif que le serveur peut envoyer à un client.

La renégociation de session peut être initiée par l'un ou l'autre côté tant que le client TLS et le serveur TLS sont autorisés à utiliser cette fonctionnalité dans le cadre de leur politique de sécurité. En cas d'échec de renégociation d'une session, la procédure de gestion des défaillances décrite dans la TLS v1.2 doit être suivie.

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 expire").

NOTE Il est prévu que le client et le serveur soient configurés avec la même politique de sécurité TLS.

Une temporisation doit être associée à la réponse à une demande de modification du cryptage. Une temporisation de la demande de modification du chiffrement doit mettre fin à la connexion. La valeur de la temporisation doit être configurable.

Pour éviter des faiblesses de la renégociation de session, l'extension de la renégociation de session définie dans la RFC 5746 doit être utilisée.

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.

5.5 Code d'authentification de message

Le code d'authentification de message doit être utilisé. Dans le cas de TLS, cette capacité est une option. La présente norme rend obligatoire l'utilisation de cette capacité pour contribuer à détecter et à contrer les attaques «man-in-the-middle». L'algorithme spécifique est indiqué par la suite chiffrée.

5.6 Prise en charge du certificat

5.6.1 Autorités de certification multiples (CA, *Certification Authorities*)

Une mise en œuvre revendiquant la conformité à la présente norme doit prendre en charge plusieurs *ancres de confiance relatives aux* autorités de certification. Le nombre réel est censé être déclaré dans la déclaration des PIXIT de la mise en œuvre.

Les critères et la sélection d'une CA ne relèvent pas du domaine d'application de la présente norme.

Dans les cas où plusieurs certificats X.509 (et la clé privée correspondante) sont disponibles sur un IED (dispositif électronique intelligent, *intelligent electronic device*), il peut être souhaitable de permettre au demandeur de choisir un certificat du côté IED qui correspond aux certificats approuvés («trusted anchor») (CA de base) disponibles du côté du demandeur.

L'extension d'indication de la CA de confiance, spécifiée dans la RFC 6066, permet à un client TLS de donner des informations relatives aux certificats de CA pris en charge localement car la CA de base des compagnies de services publics peut ne pas être publique. L'extension permet au demandeur d'influencer la sélection du certificat X.509 du côté IED pour l'authentification du côté serveur afin de permettre la vérification du certificat X.509 utilisé du côté demandeur.

L'indication de la CA de confiance est contenue dans le message d'accueil du client. Un serveur TLS recevant une indication de CA de confiance peut utiliser ces informations pour guider sa sélection d'une chaîne de certificats appropriée à renvoyer au client. Conformément à la RFC 6066, dans ce cas, le serveur doit inclure une extension de type "trusted_ca_keys" dans le message "server hello" (message d'accueil du serveur) (étendu). Le champ "extension_data" de cette extension doit être vide.

La prise en charge de cette extension peut s'appliquer aux cas où différents domaines administratifs ont accès aux IED, par exemple, deux centres de services publics avec leur propre infrastructure de clé publique. Si différents domaines administratifs sont à prendre en charge, l'extension d'indication de la CA approuvée TLS doit être utilisée.

Les mises en œuvre revendiquant la conformité à la présente norme utilisant cette extension doivent spécifier la sélection des certificats émis par la CA demandés du côté serveur TLS. Il est nécessaire de le spécifier pour les cas de succès et d'échec d'un certificat correspondant émis par la CA. Spécifier les contraintes de traitement de l'indication de la CA de confiance relève des PIXIT de la norme de référence.

~~Il convient que la défaillance d'un certificat correspondant émis par la CA entraîne un événement de sécurité ("incident: CA non trouvée"). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.~~

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

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

5.6.2 Taille de certificat

Un protocole spécifiant l'utilisation de la présente norme doit spécifier la taille maximale du certificat dont l'utilisation est autorisée. La recommandation en la matière stipule que cette taille doit être inférieure ou égale à 8 192 octets.

NOTE 1 Le certificat peut aussi comporter des informations relatives au rôle, conformément à l'IEC TS 62351-8, qui influencent sa taille finale.

NOTE 2 La taille du certificat peut être influencée par la sélection attentive des noms des émetteurs, des domaines et des extensions prises en charge, etc.

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

L'échange et la validation de certificats doivent être bidirectionnels pour obtenir l'authentification réciproque. Si une entité ne fournit pas son certificat, la connexion doit prendre fin.

NOTE 1 Le certificat serveur est transmis dans le message *ServerHello*. Le certificat client est transmis dans le message *Certificate*.

~~Il convient que l'arrêt de la connexion dû à l'absence de certificat de l'un ou l'autre côté entraîne un événement de sécurité («incident: certificat non disponible»). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.~~

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").

NOTE 2 L'option consistant à contrôler les événements de sécurité à distance est préférentielle.

5.6.4 Validation de certificat de clé publique

5.6.4.1 Généralités

Les certificats doivent être validés à la fois par les nœuds appelants et par les nœuds appelés. Il existe deux mécanismes qui doivent être configurables pour la vérification des certificats.

- Acceptation d'un certificat d'une CA autorisée
- Acceptation de certificats individuels d'une CA autorisée

5.6.4.2 Vérification basée sur la CA

Une mise en œuvre revendiquant la conformité à la présente norme doit pouvoir être configurée pour accepter les certificats d'une ou de plusieurs autorités de certification, sans la configuration des certificats individuels.

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

Une mise en œuvre revendiquant la conformité à la présente norme doit pouvoir être configurée pour accepter les certificats individuels spécifiques d'une ou de plusieurs autorités de certification autorisées (par exemple configurée).

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

La révocation de certificat doit ~~être effectuée comme~~ suivre les paramètres et procédures obligatoires spécifiés dans l'ISO/IEC 9594-8.

La gestion de la liste de révocation de certificat (CRL) relève d'une mise en œuvre locale. L'IEC TS 62351-1 traite des questions de gestion de la CRL. En variante aux CRL locales, les OCSP peuvent être utilisés pour vérifier l'état de révocation des certificats appliqués. L'IEC ~~TS~~ 62351-9 présente l'application de l'OCSP.

Une mise en œuvre revendiquant la conformité à la présente norme doit être capable de vérifier la CRL locale selon un intervalle configurable. Le processus de vérification de la CRL ne doit pas provoquer la fin d'une session établie. Une incapacité à accéder à la CRL ne doit pas provoquer la fin d'une session.

Les certificats révoqués ne doivent pas être utilisés dans l'établissement ou la renégociation d'une session TLS. Une entité recevant un certificat révoqué au cours de l'établissement de la session doit refuser la connexion. Une entité recevant un certificat révoqué au cours de la renégociation de la session doit mettre fin à la connexion.

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").

~~La révocation d'un certificat doit mettre fin à une session établie utilisant ce certificat.~~

Les autres normes faisant référence à la présente norme doivent spécifier les intervalles d'évaluation par défaut recommandés. La norme de référence doit déterminer quelle action doit être entreprise si un certificat en cours d'utilisation a été révoqué.

A Noter que des connexions peuvent prendre fin au moyen de la distribution/application normale des CRL, créant ainsi une incapacité à communiquer. Il convient donc que les administrateurs du système développent des procédures de gestion de certificat afin de réduire le nombre d'occurrences de cet événement (voir aussi l'IEC 62351-9). Il est également prévu de mettre en place un processus de gestion de sécurité afin d'évaluer la CRL avant la distribution, et ce afin d'éviter une coupure invalide de la connexion de la communication qui peut influencer sur la fiabilité. Un dispositif peut également prendre en charge de multiples certificats pour passer à un autre certificat (valide) en cours de route.

~~Il convient que le refus / l'arrêt d'une connexion dû à un certificat révoqué entraîne un événement de sécurité («incident: certificat révoqué»). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.~~

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

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

5.6.4.5 Certificats expirés

~~L'expiration d'un certificat ne doit pas provoquer la fin des connexions.~~

~~Un certificat expiré ne doit pas être utilisé ni accepté au cours de l'établissement de la connexion ou d'une renégociation de session.~~

Les certificats expirés ne doivent pas être utilisés dans l'établissement ou la renégociation d'une session TLS. Une entité recevant un certificat expiré au cours de l'établissement de la session doit refuser la connexion. Une entité recevant un certificat expiré au cours de la renégociation de la session doit mettre fin à la connexion.

Noter qu'il est prévu de mettre en place un processus de gestion de sécurité afin d'initier une procédure de renouvellement de certificat dans les délais (voir également l'IEC 62351-9). Un exemple de délai peut être un mois. Un dispositif peut également prendre en charge de multiples certificats pour permettre de passer à un autre certificat (valide).

~~Il convient que le refus d'une connexion dû à un certificat expiré entraîne un événement de sécurité («avertissement: certificat expiré»). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les événements de sécurité.~~

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

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

5.6.4.6 Signature

La signature au moyen de l'utilisation d'algorithmes RSA ou DSS doit être prise en charge. D'autres algorithmes, par exemple ceux basés sur la cryptographie de courbe elliptique comme ECDSA ou ECGDSA peuvent être indiqués dans des normes faisant référence au présent document.

Dans le cas des signatures basées sur RSA, la longueur de clé suivante doit être prise en charge:

- ~~— Facultative: Opération de signature: RSA d'une longueur de clé de 1 024 Bits (mode hérité);~~
- Obligatoire: Opération de signature: RSA d'une longueur de clé minimale de 2 048 Bits (mode moderne).

~~La prise en charge facultative de RSA d'une longueur de clé de 1 024 bits est prévue pour la rétrocompatibilité et affecte principalement le côté récepteur. 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 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.

Un algorithme RSA de 1 024 bits n'est plus reconnu comme sécurisé par rapport à la longueur de clé et il est donc fortement recommandé d'effectuer une appréciation du risque avant utilisation de ces clés. Si des clés d'une longueur supérieure à 1 024 bits ne peuvent pas être utilisées, il est aussi recommandé de prendre des mesures de sécurité supplémentaires. L'utilisation d'un RSA de 1024 bits sera déconseillée dans la prochaine édition de la présente norme. L'IEC/TS 62351-9 donne plus d'informations sur les cycles de vie des puissances de chiffrement.

Les politiques de sécurité des entités doivent pouvoir refuser ou éviter de prendre en compte toute longueur de clé facultative.

NOTE Les recommandations concernant la longueur de clé exigée pour les algorithmes de signature sont revues constamment et peuvent être consultées dans les documents NIST SP800-57, BnetzA (BSI), ou NSA Suite B.

Opération de signature facultative: courbes elliptiques définies sur des corps finis avec un algorithme de signature ECDSA ou ECGDSA (pour ECGDSA, voir l'ISO/IEC 15946-2). La longueur de clé minimale recommandée est de 256 bits (en combinaison avec SHA-256). L'OID (identifiant d'objet, *Object Identifier*) pour ecdsa-with-SHA256 à utiliser est: iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2. Les suites chiffrées pour la TLS qui utilisent l'ECDSA sont définies dans la RFC 4492 ainsi que dans la RFC 5246.

La courbe à utiliser pour ECDSA doit être secp256r1. L'OID pour cette courbe est: iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7.

La prise en charge facultative pour ECDSA utilisant la courbe brainpoolP256r1 peut être prise en charge. L'OID pour cette courbe est: iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7).

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.

SHA-1 n'est plus reconnu comme sécurisé par rapport à la résistance à la collision et il est donc fortement recommandé d'effectuer une appréciation du risque avant d'utiliser cet algorithme. Si SHA-256 ne peut être utilisé, il est aussi recommandé de prendre des mesures de sécurité supplémentaires. L'utilisation de SHA-1 sera rejetée dans la prochaine édition de la présente norme.

Les politiques de sécurité des entités doivent pouvoir refuser ou éviter de prendre en compte tout algorithme de hachage facultatif.

NOTE Les recommandations concernant les algorithmes de hachage sécurisés sont revues constamment et peuvent être consultées dans les documents NIST SP800-57, BnetZA (BSI), ou NSA Suite B.

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

Les mécanismes de clés publiques (basés sur RSA) et les mécanismes Diffie-Hellman et Diffie-Hellman éphémères doivent être pris en charge. Dans le cas des algorithmes d'échange de clés, la longueur de clé suivante doit être prise en charge:

- ~~Facultative: Longueur de clé RSA minimale de 1 024 bits (mode hérité);~~
- Obligatoire: Longueur de clé RSA recommandée d'au moins 2 048 bits ~~(mode moderne).~~

~~La prise en charge facultative d'une longueur de clé RSA de 1 024 bits est prévue pour la rétrocompatibilité. Une longueur de clé de 2 048 bits doit être prise en charge, et il s'agit de la longueur de clé préférentielle à utiliser. Il convient que l'application des clés RSA de 1 024 bits entraîne un avertissement de sécurité («avertissement: longueur de clé minimale»). Il convient que les mises en œuvre fournissent un mécanisme pour annoncer les avertissements de sécurité.~~

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").

Une longueur de clé RSA de 1 024 bits pour l'échange de clés n'est plus reconnue comme sécurisée et il est donc fortement recommandé d'effectuer une appréciation du risque avant d'utiliser ces clés. Si une longueur de clé supérieure à 1 024 bits ne peut pas être utilisée, il est aussi recommandé de prendre des mesures de sécurité supplémentaires. L'utilisation d'une longueur de clé de 1 024 bits sera déconseillée dans la prochaine édition de la présente norme. L'IEC-~~TS~~ 62351-9 donne plus d'informations sur les cycles de vie des puissances de chiffrement.

Les politiques de sécurité des entités doivent pouvoir refuser ou éviter de prendre en compte toute longueur de clé facultative. Si l'un des mécanismes de clés publiques basés sur des courbes elliptiques est pris en charge (par exemple, ECDSA), tout comme les mécanismes Diffie-Hellman basés sur une courbe elliptique et les mécanismes Diffie-Hellman éphémères basés sur une courbe elliptique sont pris en charge, la longueur de clé suivante doit être prise en charge:

Obligatoire: Longueur de clé ECDSA minimale de 256 bits

NOTE Des suites chiffrées définies pour la prise en charge TLS ainsi qu'un mélange entre des signatures basées sur RSA et des Diffie-Hellman basés sur une courbe elliptique existent.

Les clients TLS qui utilisent la TLS version 1.2 doivent inclure l'extension `signature_algorithm` avec au moins la combinaison de {RSA, SHA-1; RSA, SHA-256; ECDSA, SHA256} dans le message *ClientHello*. D'autres combinaisons peuvent être prises en charge.

NOTE Si `signature_algorithm` n'est pas incluse, le serveur TLS 1.2 revient par défaut, c'est-à-dire SHA-1.

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.

SHA-1 n'est plus reconnu comme sécurisé par rapport à la résistance à la collision et il est donc fortement recommandé d'effectuer une appréciation du risque avant d'utiliser cet algorithme. Si SHA-256 ne peut être utilisé, il est aussi recommandé de prendre des mesures de sécurité supplémentaires. L'utilisation de SHA-1 sera rejetée dans la prochaine édition de la présente norme.

Les politiques de sécurité des entités doivent pouvoir refuser ou éviter de prendre en compte tout algorithme de hachage facultatif.

NOTE Les recommandations concernant les algorithmes de hachage sécurisé sont revues constamment et peuvent être consultées dans les documents NIST SP800-57, BnetzA (BSI), ou NSA Suite B.

5.7 Coexistence avec un trafic de protocole non sécurisé

Les normes de référence doivent fournir un port TCP/IP séparé par lequel échanger un trafic sécurisé TLS. Cela donne la possibilité d'établir simultanément des communications sécurisées non ambiguës et des communications non sécurisées.

6 Prise en charge de mesures de sécurité – facultatif

Dans certains déploiements, une prise en charge supplémentaire est nécessaire pour limiter davantage l'utilisation de certificats sur la base de leurs numéros de série et de leurs émetteurs. Cette limitation est matérialisée par une liste blanche de certificats ou un marquage de certificats qui est en cours de définition par l'IETF (*Internet Engineering Task Force*). Une liste blanche de certificats peut être prise en charge de façon facultative. Si une mise en œuvre prend en charge la liste blanche de certificats, une liste blanche doit être élaborée en indiquant le numéro de série et l'émetteur des certificats autorisés. Cette méthode n'étant pas limitée à l'utilisation de certificats en TLS, elle est traitée plus en détail dans l'IEC TS 62351-9.

7 Exigences relatives aux normes de référence

Les autres normes faisant référence à la présente norme doivent spécifier:

- Les suites chiffrées TLS obligatoires à prendre en charge.
- Si des versions autres que la TLS 1.2 doivent être utilisées, la norme de référence doit définir les versions exigées.
- ~~– La période recommandée au cours de laquelle les clés de chiffrement doivent être échangées (mise à jour de la clé de session).~~
- La spécification recommandée concernant la méthode de reprise ~~des clés~~ de session et les paramètres provenant d'une connexion antérieure sur la base ~~du trafic de protocole et/ou~~ de la durée d'exécution de la session. ~~Cette spécification doit indiquer le mécanisme permettant de mesurer le trafic (par exemple, les paquets envoyés, les octets envoyés, etc.) et la métrique recommandée selon laquelle il convient d'effectuer la reprise de session.~~ Notez que cette durée ne doit pas excéder 24 h.
- La spécification recommandée concernant la renégociation des ~~clés~~ paramètres de session sur la base ~~du trafic de protocole et/ou~~ de la durée d'exécution de la session. ~~Cette spécification doit indiquer le mécanisme permettant de mesurer le trafic (par exemple, les paquets envoyés, les octets envoyés, etc.) et la métrique recommandée selon laquelle il convient d'effectuer la renégociation de session.~~ Il convient qu'une renégociation de session soit toujours cohérente avec la période de rafraîchissement de la CRL, afin d'éviter des vérifications inutiles de la révocation de certificat.
- Les champs de certificat individuel, si la validation de certificat doit être limitée aux certificats dédiés d'une CA autorisée (au lieu d'autoriser tous les certificats).
- Le nombre recommandé de CA à prendre en charge.
- Le port TCP à utiliser afin de différencier le trafic de communications sécurisées (par exemple, utilisant TLS) et non sécurisées.
- La taille maximale ~~de~~ du certificat de clé publique.
- La période par défaut recommandée d'évaluation de ~~la CRL~~ révocation de certificat.
- ~~Dans le cas où~~ Si un OCSP est utilisé pour les vérifications de révocation de certificat, le traitement des défaillances pour accéder au répondeur OCSP.
- La gestion des actions de ~~révocation~~ validation de certificat par rapport aux certificats utilisés dans le contexte de la TLS, ~~puisque la révocation ou l'expiration d'un certificat influence la sécurité de la connexion.~~ Des mesures appropriées doivent être spécifiées afin de garantir la disponibilité du système et du service.
- La gestion des événements de sécurité définis dans la présente partie.
- Le niveau ~~requis~~ exigé de conformité à la présente norme.

8 Conformité

~~La conformité à la présente partie de l'IEC 62351 doit être déterminée par l'application de toutes les parties de l'Article 5.~~

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.

Tableau 1 – Conformité aux suites chiffrées TLS

Suite chiffrée	Client		Serveur		Valeur/Observation
	F/S	Déclaré	F/S	Déclaré	
TLS_NULL_WITH_NULL_NULL	x		x		
TLS_RSA_WITH_NULL_MD5	x		x		
TLS_RSA_WITH_NULL_SHA	f		f		SHA-1 déconseillé
TLS_RSA_WITH_NULL_SHA256	f		f		

Noter que le 5.1 autorise également d'autres suites chiffrées pour la prise en charge de l'intégrité uniquement. De plus, des suites chiffrées spécifiques considérées comme obligatoires ou facultatives seront spécifiées par la norme de référence.

8.4 Conformité aux versions TLS sélectionnées

Le Tableau 2 indique les exigences de conformité pour les versions TLS, définies en 5.2.

Tableau 2 – Conformité aux versions TLS

Version TLS	Client		Serveur		Valeur/Observation
	F/S	Déclaré	F/S	Déclaré	
1,0	f		f		Faiblesses connues, uniquement pour la rétrocompatibilité
1,1	f		f		Faiblesses connues, uniquement pour la rétrocompatibilité
1,2	o		o		
1,3	f		f		Toutes les caractéristiques ne sont pas spécifiées dans le présent document

8.5 Conformité aux caractéristiques de protocole TLS sélectionnées

Le Tableau 3 indique les exigences de conformité pour les versions TLS, définies en 5.3, 5.4 et 5.6.

Tableau 3 – Conformité aux caractéristiques de protocole TLS

Caractéristique TLS	Client		Serveur		Valeur/Observation
	F/S	Déclaré	F/S	Déclaré	
Reprise de session TLS au moins toutes les 24 h	o		o		
Lancement d'une reprise de session TLS en utilisant ClientHello	o		x		
Lancement d'une reprise de session TLS en utilisant HelloRequest	x		o		
Reprise de session TLS en utilisant des tickets de session	f		f		selon RFC 5077
Renégociation de session TLS au moins toutes les 24 h	o		o		
Lancement d'une renégociation de session TLS en utilisant ClientHello	o		x		
Lancement d'une renégociation de session TLS en utilisant HelloRequest	x		o		
Extension de la renégociation de session TLS	o		o		selon RFC 5746
Prise en charge de l'extension de la CA de confiance (RFC 6066)	f		f		

8.6 Conformité à la prise en charge des certificats

Le Tableau 4 indique les exigences de conformité pour la prise en charge des certificats, définies en 5.6 et à l'Article 6.

Tableau 4 – Conformité à la prise en charge des certificats

	Client		Serveur		Valeur/Observation
	F/S	Déclaré	F/S	Déclaré	
Prise en charge de CA multiples (certificats de base)	f		f		Norme de référence définie
La taille maximale du certificat prise en charge est de 8 192 octets	o		o		A examiner?
Application des règles de validation de certificat conformément à la RFC 5280 (validité, signature de la CA, état de révocation, etc.)	o		o		
Validation de l'état de révocation des certificats à l'aide de la CRL	o		o		Période d'évaluation à spécifier par la norme de référence.
Validation de l'état de révocation des certificats à l'aide de l'OCSP	f		f		
Élaboration d'une liste blanche de certificats selon l'IEC 62351-9	f		f		

8.7 Conformité à la prise en charge des algorithmes cryptographiques

Le Tableau 5 indique les exigences de conformité pour la prise en charge des certificats, définies en 5.6.4.6 et 5.6.4.7.

Tableau 5 – Conformité à la prise en charge des algorithmes cryptographiques

Algorithmes de signature et de hachage	Client		Serveur		Valeur/Observation
	F/S	Déclaré	F/S	Déclaré	
Prise en charge de RSA 2048	o		o		
Prise en charge de RSA 1024	f		f		déconseillée
Prise en charge de ECDSA avec des clés de 256 bits, OID (identifiant d'objet): 1.2.840.10045.4.3.2; Prise en charge de la courbe secp256r1, OID: 1.2.840.10045.3.1.7	f		f		
Prise en charge de ECGDSA avec des clés de 256 bits, OID: 1.3.36.3.3.2.5.4.4; Prise en charge de la courbe brainpoolP256r1, OID: 1.3.36.3.3.2.8.1.1.7	f		f		
Prise en charge de SHA-256	o		o		
Prise en charge de SHA-1	f		f		déconseillée
Prise en charge de MD5	x		x		

Bibliographie

ISO/IEC 15946-2, *Technologies de l'information – Techniques de sécurité – Techniques cryptographiques basées sur les courbes elliptiques – Partie 2: Signatures digitales* (supprimée)

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

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control* (disponible en anglais seulement)

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Events Logs* (disponible en anglais seulement)³

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* (disponible en anglais seulement)

NIST SP-800-57 Part 1 Rev. 3, *Recommendations for Key Management*, juillet 2012 (disponible en anglais seulement)

BNetzA, BSI, *Algorithms for Qualified Electronic Signatures*, 02/2013 (disponible en anglais seulement)

NSA Suite B, *Suite B Cryptography / Cryptographic Interoperability* (disponible en anglais seulement)

³ En cours de préparation. Stade au moment de la publication: IEC/PCC 62351-14:2020.

FINAL VERSION

VERSION FINALE



**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**

CONTENTS

FOREWORD	3
INTRODUCTION to Amendment 2	5
1 Scope	6
1.1 Scope	6
1.2 Intended Audience	6
2 Normative references	6
3 Terms, definitions and abbreviations	7
3.1 Terms, definitions and abbreviations	7
3.2 Additional abbreviations	7
4 Security issues addressed by this standard	7
4.1 Operational requirements affecting the use of TLS in the telecontrol environment	7
4.2 Security threats countered	8
4.3 Attack methods countered	8
4.4 Handling of security events	8
5 Mandatory requirements	9
5.1 Deprecation of cipher suites	9
5.2 Negotiation of versions	9
5.3 Session resumption	10
5.4 Session renegotiation	11
5.5 Message Authentication Code	12
5.6 Certificate support	12
5.7 Co-existence with non-secure protocol traffic	16
6 Optional security measure support	16
7 Referencing standard requirements	16
8 Conformance	17
8.1 General	17
8.2 Notation	17
8.3 Conformance to selected cipher suites	17
8.4 Conformance to selected TLS versions	17
8.5 Conformance to selected TLS protocol features	17
8.6 Conformance to certificate support	18
8.7 Conformance to cryptographic algorithm support	18
Bibliography	20
Table 1 – Conformance to TLS cipher suites	17
Table 2 – Conformance to TLS versions	17
Table 3 – Conformance to TLS protocol features	18
Table 4 – Conformance to certificate support	18
Table 5 – Conformance to cryptographic algorithm support	19

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendments has been prepared for user convenience.

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

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

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

The committee has decided that the contents of the base publication and its amendments will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

INTRODUCTION to Amendment 2

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

- Support for TLS versions 1.1 and 1.0 is made optional instead of mandatory to address known weaknesses. This is aligned with the defined security warnings for TLS versions 1.1 and 1.0.
- Update of TLS version handling during renegotiation and resumption to avoid TLS version downgrade/upgrade within a same session.
- Updated explanatory text for session renegotiation to make the communication relations clearer.
- Deprecation of RSA1024 and SHA-1 algorithms. This underlines the desire to disallow them in the next edition.
- Inclusion of PICS section for mandatory and optional settings in TLS.
- Updated text for and enhancements of security events to better align with IEC 62351-14
- Inclusion of general remarks for the security event handling.
- Update of references.

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

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

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

1 Scope

1.1 Scope

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

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

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

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

1.2 Intended Audience

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

RFC 6066:2006, *Transport Layer Security Extensions*

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

3 Terms, definitions and abbreviations

3.1 Terms, definitions and abbreviations

For the purposes of this document, the terms, definitions and abbreviations given in IEC TS 62351-2, Glossary, apply.

3.2 Additional abbreviations

CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
ECDSA	Elliptic Curve Digital Signature Algorithm
ECGDSA	Elliptic Curve German Digital Signature Algorithm (see ISO/IEC 15946-2)
OCSP	Online Certificate Status Protocol (see RFC 6960)
PIXIT	Protocol Implementation eXtra Information for Testing

4 Security issues addressed by this standard

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

The IEC telecontrol environment has different operational requirements from many Information Technology (IT) applications that make use of TLS in order to provide security protection. The most differentiating, in terms of security, is the duration of the TCP/IP connection for which security needs to be maintained.

Many IT protocols have short duration connections, which allow the encryption algorithms to be renegotiated at connection re-establishment. However, the connections within a telecontrol environment tend to have longer durations, often “permanent”. It is the longevity of the connections in the field of power systems management and associated information exchange that give rise to the need for special consideration. In this regard, in order to provide protection for the “permanent” connections, a mechanism for updating the session key is specified within this standard, based upon the TLS features of session resumption and

¹ This is typically referred to as SSL/TLS.

session re-negotiation while also considering the relationship with certificate revocation state information.

Another issue addressed within this standard is how to achieve interoperability between different implementations. TLS allows for a wide variety of cipher suites to be supported and negotiated at connection establishment. However, it is conceivable that two implementations could support mutually exclusive sets of cipher suites. This standard specifies that referring standards must specify at least one common cipher suite and a set of TLS parameters that allow interoperability.

Additionally, this standard specifies the use of particular TLS capabilities that allow for specific security threats to be countered.

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).

NOTE It is intended that certificate management necessary to operate TLS be specified in compliance with IEC TS 62351-9.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

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.

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

The specific threats countered in this part of IEC 62351 for the transport layers include:

- Unauthorized modification or insertion of messages through message level authentication and integrity protection of messages.

Additionally, when the information has been identified as requiring confidentiality protection:

- Unauthorized access or theft of information through message level encryption of the messages

4.3 Attack methods countered

The following security attack methods are countered through the appropriate implementation of the specifications and recommendations in this part of IEC 62351.

- Man-in-the-middle: This threat is countered through the use of a Message Authentication Code mechanism or digital signatures specified within this document.
- Replay: This threat is countered through the use of specialized processing state machines specified by the normative references of this document.
- Eavesdropping: This threat is countered through the use of encryption.

NOTE The actual performance characteristics of an implementation claiming conformance to this standard are out-of-scope of this standard.

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

Any cipher suite that specifies NULL for encryption shall not be used for communication outside the administrative domain, if the encryption of this communication connection by other means cannot be guaranteed.

NOTE 1 This standard does not exclude the use of encrypted communications through the use of cryptographic based VPN tunnels. The use of such VPNs is out-of-scope of this standard.

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

- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256

NOTE 2 The application of no-encrypting cipher suites allows for traffic inspection while still retaining an end-to-end authentication and integrity protection of the traffic.

Implementations allowing TLS cipher suites with NULL encryption claiming conformance to this part shall provide a mechanism to explicitly enable those TLS cipher suites. Per default, non-encrypting TLS cipher suites are not allowed.

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.

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.

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

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_WITH_NULL_MD5

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

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.

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").

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

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 5246). 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 leading to a smaller session resumption interval than the session renegotiation interval. ($0 < \text{session resumption interval} < \text{session renegotiation interval} \leq 24\text{h}$).

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 PICS 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.

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

5.4 Session renegotiation

Session renegotiation in TLS requires a complete TLS handshake where all asymmetric operations and certificate checks must be performed. Session renegotiation will result in a completely new session based upon both a freshly negotiated master key and a new session key. During the TLS handshake phase, the certificates are also checked for their validity and their revocation state. Hence, the timeframe for session renegotiation should be chosen in accordance to the refresh of the revocation state information (CRL) as described in 5.6.4.4.

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 $\frac{1}{2}$ CRL refresh time or $\frac{1}{2}$ 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 PICS of the referencing standard.

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 send 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 (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").

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

There shall be a timeout associated with the response to a change cipher request. A timeout of the change cipher request shall result in the connection being terminated. The timeout value shall be configurable.

To avoid weaknesses in session renegotiation, the session renegotiation extension defined in RFC 5746 shall be used.

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.

5.5 Message Authentication Code

The Message Authentication Code shall be used. TLS has this capability specified as an option. This standard mandates the use of this capability to aid in countering and detecting man-in-the-middle attacks. The specific algorithm is indicated by the cipher suite.

5.6 Certificate support

5.6.1 Multiple Certification Authorities (CAs)

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

The criteria and selection of a CA is out-of-scope of this standard.

In scenarios where more than one X.509 certificate (and corresponding private key) is available on an IED, it may be desirable to enable the requester to choose a certificate on the IED side that matches the trusted anchor (root CA) certificates available at the requester side.

The Trusted CA Indication extension specified in RFC 6066 allows a TLS client to provide information about locally supported CA certificates since the root CA of the utilities may not be public. The extension allows the requesting party to influence the selection of the X.509 certificate on the IED side for the server side authentication to enable the verification of the used X.509 certificate on the requestor side.

The Trusted CA Indication is contained in the client hello message. A TLS server receiving a Trusted CA Indication may use this information to guide its selection of an appropriate certificate chain to return to the client. According to RFC 6066 in this event, the server shall include an extension of type "trusted_ca_keys" in the (extended) server hello. The "extension_data" field of this extension shall be empty.

The support of this extension may be applicable in scenarios where IEDs are accessed by different administrative domains, e.g., two utilities with an own public key infrastructure. If different administrative domains are to be supported, the TLS Trusted CA Indication extension shall be used.

Implementations claiming conformance to this standard using this extension shall specify the selection of the requested CA issued certificates on the TLS server side. This needs to be specified for the success and failure case of a matching CA issued certificate. It is a PIXIT issue, of the referencing standard, to specify the constraints on the Trusted CA Indication handling.

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

NOTE The option to remotely monitor security events is preferred.

5.6.2 Certificate size

A protocol specifying the use of this standard shall specify the maximum size of certificate allowed to be used. It is recommended that this size shall be less than or equal to 8 192 octets.

NOTE 1 The certificate may also carry role information according to IEC TS 62351-8, which influences its final size.

NOTE 2 The certificate size may be influenced by the careful selection of names in issuer and subject field and supported extensions, etc.

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

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 shall raise a security event ("alarm: certificate unavailable").

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

5.6.4 Public-key certificate validation

5.6.4.1 General

Certificates shall be validated by both the calling and called nodes. There are two mechanisms that shall be configurable for certificate verification.

- Acceptance of any certificate from an authorized CA
- Acceptance of individual certificates from an authorized CA

5.6.4.2 Verification based upon CA

An implementation claiming conformance to this standard shall be capable of being configured to accept certificates from one or more Certificate Authorities without the configuration of individual certificates.

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

An implementation claiming conformance to this standard shall be capable of being configured to accept specific individual certificates from one or more authorized Certificate Authorities (e.g. configured).

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

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.

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")."

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 shall raise a security event ("alarm: revoked certificate").

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

5.6.4.5 Expired certificates

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 shall raise a security event ("alarm: expired certificate").

NOTE The option to remotely monitor security events is preferred.

5.6.4.6 Signing

Signing through the use of RSA or DSS algorithms shall be supported. Other algorithms, e.g., those based on elliptic curve cryptography like ECDSA or ECGDSA may be specified in standards that reference this document.

For RSA-based signatures, the following key length shall be supported:

- Mandatory: Signature-operation: RSA with a key length of at least 2 048 Bits.

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.

1 024 bits RSA is no longer recognized as secure with respect to the key length and it is therefore strongly recommended to perform a risk assessment before using these keys. If longer keys than 1 024 bits cannot be used, it is also recommended that additional security measures be taken. The usage of 1 024 bit RSA will be deprecated in the next edition of this standard. IEC/TS 62351-9 will provide 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.

NOTE Recommendations regarding required key length for signature algorithms are reviewed constantly and can be found in NIST SP800-57, BnetZA (BSI), or the NSA Suite B.

Optional Signature-operation: Elliptic curves defined over finite prime fields with signature algorithm ECDSA or ECGDSA (for ECGDSA, see ISO/IEC 15946-2). The recommended minimum key length is 256 bits (in combination with SHA-256). The OID to for ecdsa-with-SHA256 to be used is: iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2. Cipher suites for TLS, which utilize ECDSA are defined in RFC 4492 as well as in RFC 5246.

The curve to be used for ECDSA shall be secp256r1. The OID for this curve is: iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7.

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 deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash 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.

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

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:

- Mandatory: Recommended RSA key length of at least 2048 Bit.

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").

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 deprecated. Its use is limited to backward compatibility. SHA-256 shall be supported and is the preferred hash 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.

5.7 Co-existence with non-secure protocol traffic

Referencing standards shall provide a separate TCP/IP port through which to exchange TLS secured traffic. This will allow for the possibility of un-ambiguous secure and non-secure communications simultaneously.

6 Optional security measure support

In certain deployments, additional support is necessary to further restrict the usage of certificates based on their serial numbers and issuers. This restriction is known as certificate white listing or certificate pinning, and is currently being defined in the IETF. Certificate white listing can be optionally supported. If an implementation supports certificate white listing, a white list shall be built by stating the serial number and the issuer of the allowed certificates. As this approach is not restricted to the usage of certificates in TLS, it is further specified in IEC TS 62351-9.

7 Referencing standard requirements

Other standards referencing this standard shall specify:

- The mandatory TLS cipher suites to be supported.
- If other versions than TLS 1.2 are to be used, the referencing standard shall define the required versions.
- 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.

8 Conformance

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		

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		

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

Bibliography

ISO/IEC 15946-2, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures* (withdrawn)

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

IEC TS 62351-8:2011, *Power systems management and associated information exchange Data and communications security – Part 8: Role-based access control*

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Events Logs*²

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

NIST SP-800-57 Part 1 Rev. 3, *Recommendations for Key Management*, July 2012

BNetzA, BSI, *Algorithms for Qualified Electronic Signatures*, 02/2013.

NSA Suite B, *Suite B Cryptography / Cryptographic Interoperability*

² Under preparation. Stage at the time of publication: IEC/PCC 62351-14:2020.

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

SOMMAIRE

AVANT-PROPOS	23
INTRODUCTION à l'Amendement 2	25
1 Domaine d'application	26
1.1 Domaine d'application	26
1.2 Utilisateurs prévus	26
2 Références normatives	27
3 Termes, définitions et abréviations	27
3.1 Termes, définitions et abréviations	27
3.2 Autres abréviations	27
4 Problèmes de sécurité couverts par la présente norme	28
4.1 Influence des exigences fonctionnelles sur l'utilisation de la TLS dans l'environnement de téléconduite	28
4.2 Menaces à la sécurité contrées	28
4.3 Méthodes d'attaques contrées	29
4.4 Gestion des événements de sécurité	29
5 Exigences obligatoires	30
5.1 Rejet de suites chiffrées	30
5.2 Négociation des versions	30
5.3 Reprise de session	31
5.4 Renégociation de session	32
5.5 Code d'authentification de message	33
5.6 Prise en charge du certificat	33
5.7 Coexistence avec un trafic de protocole non sécurisé	38
6 Prise en charge de mesures de sécurité – facultatif	38
7 Exigences relatives aux normes de référence	39
8 Conformité	39
8.1 Généralités	39
8.2 Notation	39
8.3 Conformité aux suites chiffrées sélectionnées	39
8.4 Conformité aux versions TLS sélectionnées	40
8.5 Conformité aux caractéristiques de protocole TLS sélectionnées	40
8.6 Conformité à la prise en charge des certificats	41
8.7 Conformité à la prise en charge des algorithmes cryptographiques	41
Bibliographie	42
Tableau 1 – Conformité aux suites chiffrées TLS	40
Tableau 2 – Conformité aux versions TLS	40
Tableau 3 – Conformité aux caractéristiques de protocole TLS	40
Tableau 4 – Conformité à la prise en charge des certificats	41
Tableau 5 – Conformité à la prise en charge des algorithmes cryptographiques	41

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

Cette version consolidée de la Norme IEC officielle et de ses amendements a été préparée pour la commodité de l'utilisateur.

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

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

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

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de la publication de base et de ses amendements ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

IECNORM.COM : Click to view the full PDF of IEC 62351-3:2014+AMD1:2018+AMD2:2020 CSV

INTRODUCTION à l'Amendement 2

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

- Prise en charge des versions TLS 1.1 et 1.0 rendue facultative plutôt qu'obligatoire pour remédier aux faiblesses connues. Cette possibilité permet de s'aligner sur les avertissements de sécurité définis pour les versions TLS 1.1 et 1.0.
- Mise à jour de la gestion des versions TLS lors de la renégociation et de la reprise pour éviter une mise à niveau inférieur/supérieur des versions TLS au cours d'une même session.
- Mise à jour du texte explicatif de la renégociation de session pour clarifier davantage les relations de communication.
- Rejet des algorithmes RSA1024 et SHA-1. Cette démarche souligne la volonté de les interdire dans la prochaine édition.
- Inclusion de la section des PICS pour les paramètres obligatoires et facultatifs dans la TLS.
- Mise à jour du texte et améliorations des événements de sécurité pour mieux s'aligner sur l'IEC 62351-14.
- Inclusion de remarques générales sur la gestion des événements de sécurité.
- Mise à jour des références.

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