

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 It also gives information on projects, replaced and withdrawn publications.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.

<https://standards.csi.csi.ch/standards/iec/2009eb5-78b8-44d9-9adf-cc7fb84efbda/iec-62351-3-2014>

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.**

Withdrawn

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

IEC 62351-3:2014

<https://standards.iteh.ai/en/standards/iec/59009eb5-78b8-44d9-9adf-cc7fb84efbda/iec-62351-3-2014>

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

<https://standards.iec.org/standards/iec/39009eb5-78b8-44d9-9adf-cc7fb84efbda/iec-62351-3-2014>

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.

iTech Standards
(<https://standards.itih.ai>)
Document Preview

IEC 62351-3:2014

<https://standards.itih.ai/standards/iec/59009eb5-78b8-44d9-9adf-ce7fb84efbda/iec-62351-3-2014>

WITHDRAWN

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.

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC 62351-3:2014](https://standards.iteh.ai/standards/iec/59009eb5-78b8-44d9-9adf-ce7fb84efbda/iec-62351-3-2014)

<https://standards.iteh.ai/standards/iec/59009eb5-78b8-44d9-9adf-ce7fb84efbda/iec-62351-3-2014>

WITHDRAWN

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-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 ~~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 ~~PIXIT~~ 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.