

# 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 © 2014 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  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

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

### About IEC publications

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

#### IEC Catalogue - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

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

#### IEC publications search - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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](http://webstore.iec.ch/justpublished)

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

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://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: [csc@iec.ch](mailto:csc@iec.ch).

### A propos de l'IEC

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

### A propos des publications IEC

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

#### Catalogue IEC - [webstore.iec.ch/catalogue](http://webstore.iec.ch/catalogue)

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

#### Recherche de publications IEC - [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

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](http://webstore.iec.ch/justpublished)

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

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [csc@iec.ch](mailto:csc@iec.ch).

# 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 978-2-8322-1900-3

**Warning! Make sure that you obtained this publication from an authorized distributor.  
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

# CONTENTS

FOREWORD .....	3
1 Scope .....	5
1.1 Scope .....	5
1.2 Intended Audience .....	5
2 Normative references .....	5
3 Terms, definitions and abbreviations .....	6
3.1 Terms, definitions and abbreviations .....	6
3.2 Additional abbreviations .....	6
4 Security issues addressed by this standard .....	6
4.1 Operational requirements affecting the use of TLS in the telecontrol environment .....	6
4.2 Security threats countered .....	7
4.3 Attack methods countered .....	7
5 Mandatory requirements .....	7
5.1 Deprecation of cipher suites .....	7
5.2 Negotiation of versions .....	8
5.3 Session resumption .....	8
5.4 Session renegotiation .....	8
5.5 Message Authentication Code .....	9
5.6 Certificate support .....	9
5.6.1 Multiple Certification Authorities (CAs) .....	9
5.6.2 Certificate size .....	10
5.6.3 Certificate exchange .....	10
5.6.4 Public-key certificate validation .....	10
5.7 Co-existence with non-secure protocol traffic .....	12
6 Optional security measure support .....	12
7 Referencing standard requirements .....	12
8 Conformance .....	13
Bibliography .....	14

ITU STANDARD PREVIEW  
 (standards.iteh.ai)

[IEC 62351-3:2014](https://standards.iteh.ai/catalog/standards/sist/39009eb5-7868-44d9-9adf/iec-62351-3-2014)

<https://standards.iteh.ai/catalog/standards/sist/39009eb5-7868-44d9-9adf/iec-62351-3-2014>

[cc71b84c1bda/iec-62351-3-2014](https://standards.iteh.ai/catalog/standards/sist/39009eb5-7868-44d9-9adf/iec-62351-3-2014)

## 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.

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

This standard cancels and replaces IEC TS 62351-3:2007.

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

FDIS	Report on voting
57/1498/FDIS	57/1515/RVD

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

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

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

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

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

## **iTeh STANDARD PREVIEW (standards.iteh.ai)**

[IEC 62351-3:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/39009eb5-78b8-44d9-9adf-ce7fb84efbda/iec-62351-3-2014>

# 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 TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management*<sup>1</sup>

ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory: 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*<sup>2</sup>

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 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

<sup>1</sup> Under consideration.

<sup>2</sup> This is typically referred to as SSL/TLS.



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). This part of IEC 62351 does not cover security for the communication application layers (OSI layers 5 and above) or application-to-application security.

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 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.

## 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

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

- TLS\_NULL\_WITH\_NULL\_NULL
- TLS\_RSA\_NULL\_WITH\_NULL\_MD5

## 5.2 Negotiation of versions

TLS v1.2 as defined in RFC 5246 (sometimes referred to as SSL v3.3) or higher shall be supported. To ensure backward compatibility implementations shall also 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).

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

NOTE The option to remotely monitor security events is preferred.

## 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). This specification follows this approach. Session resumption should be performed in less than 24 hours, 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.

Implementations claiming conformance to this standard shall specify that the symmetric session keys to be renewed within the maximum time period and maximum allowed number of packets/bytes sent. These resumption maximum time/bytes constraints are expected to be specified in a PIXIT of the referencing standard. The maximum time period for session resumption shall be aligned with the CRL refresh time.

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

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

## 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.

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 renegotiation maximum time/bytes constraints are expected to be specified in a PIXIT (Protocol Implementation eXtra Information for Testing) of the referencing standard.

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 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.

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.

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.

## 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.

## 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. 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 a matching CA issued certificate should raise a security event ("incident: CA 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.

### 5.6.3 Certificate exchange

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

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

NOTE 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.

#### 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).

#### 5.6.4.4 Certificate revocation

Certificate revocation shall be performed as 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 of a session. An entity receiving a revoked certificate during session establishment shall refuse the connection.

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.