TECHNICAL SPECIFICATION

IEC TS 62351-3

First edition
2007-06

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

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

Reference number
IEC/TS 62351-3:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

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

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

TECHNICAL SPECIFICATION

IEC TS 62351-3

First edition
2007-06

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

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE K

For price, see current catalogue

CONTENTS

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-3, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/803/DTS	57/857/RVC

Full information on the voting for the approval of this technical specification 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 of 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 maintenance result 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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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

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

1 Scope and object

1.1 Scope

This part of IEC 62351, which is a technical specification, specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer.

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 outside the scope of this technical specification.

1.2 Object

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 2246) so that they are applicable to the telecontrol environment of IEC TC 57. It is intended that this specification be referenced as a normative part of other IEC TC 57 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 technical specification is to be referenced.

This part reflects the security requirements of the IEC TC 57 protocols. Should other standards bring forward new requirements, this specification may need to be revised.

The initial audience for this specification is intended to be the members of the working groups developing or making use of the protocols within IEC TC 57. 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. This specification 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

RFC 2246:1999, *The TLS Protocol Version 1.0*[1)]

RFC 2712:1999, *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*[2)]

RFC 3268, 2002, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*

RFC 3280, 2002, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

3 Terms and definitions

For the purposes of this document, the terms and definitions contained in IEC 62351-2 apply.

4 Security issues addressed by this technical specification

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

The IEC TC 57 telecontrol environment has different operational requirements than many information technology (IT) protocols 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 IEC/TC 57 connections that give rise to the need for special consideration. In this regard, in order to provide confidentiality for the “permanent” connections, a transparent mechanism for encryption key re-negotiation is specified within this technical specification.

Another issue addressed within this specification 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 technical specification specifies that referring standards must specify at least one common cipher suite and a set of TLS parameters that allow interoperability.

---

1) T. Dierks, C. Allen. This standard is typically referred to as SSL/TLS.

2) A. Medvinsky, M. Hur.

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

4.2 Security threats countered

See IEC 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). This part 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 for the transport layers include:

– unauthorized access to information through message level authentication and encryption of the messages;

– unauthorized modification (tampering) or theft of information through message level authentication and 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:

– 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 in RFC 2246, RFC 2712 and RFC 3268;

– eavesdropping: this threat is countered through the use of encryption.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this specification.

5 Mandatory requirements

5.1 Deprecation of non-encrypting cipher suites

Any cipher suite that specifies NULL for encryption shall not be used.

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

TLS_NULL_WITH_NULL_NULL;

TLS_RSA_NULL_WITH_NULL_MD5;

TLS_RSA_NULL_WITH_NULL_SHA.

5.2 Negotiation of versions

Only TLS 1.0 corresponding to SSL version 3.1 (or higher) shall be allowable. Proposal of version prior to SSL 3.1 shall result in no connection being established.

5.3 Cipher renegotiation

Implementations claiming conformance to this technical specification shall specify that the symmetric keys shall be renegotiated based upon a time period and a maximum allowed number of packets/bytes sent. It is a PIXIT (Protocol Implementation eXtra Information for Testing) issue, of the referencing standard, to specify the constraints on the renegotiation.

The renegotiation values shall be configurable.

The initiation of the change cipher 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.

5.4 Message authentication code

The message authentication code shall be used.

NOTE TLS has this capability specified as an option. This technical specification mandates the use of this capability to aid in countering and detection of man-in-the-middle attacks.

5.5 Certificate support

5.5.1 Multiple Certificate Authorities (CAs)

An implementation claiming conformance to this technical specification shall support more than one Certificate Authority. The actual number shall be declared in the implementation's PIXIT statement.

The criteria and selection of a CA are out-of-scope of this technical specification.

5.5.2 Certificate size

A protocol specifying the use of this technical specification shall specify the maximum size of certificate allowed to be used. It is recommended that this size shall be less than or equal to 8192 bytes.

5.5.3 Certificate exchange

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

5.5.4 Certificate comparison

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.

5.5.4.1 Verification based upon CA

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

5.5.4.2 Verification based upon individual certificates

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

5.5.4.3 Certificate revocation

Certificate revocation shall be performed as specified in RFC 3280.

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 62351-1.

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

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

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

Other standards referencing this technical specification 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 Through the normal application/distribution of CRL(s) connections may be terminated creating an inability to perform communications. Thus system administrators should develop certificate management procedures to mitigate such an occurrence.

5.5.4.4 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.

5.5.4.5 Signing

Signing through the use of RSA or DSS algorithms shall be supported. Other algorithms may be specified in standards that reference this document.

5.5.4.6 Key exchange

The key exchange algorithms shall support a maximum size of at least 1024 bits for the key.

Both RSA and Diffe-Hellman mechanisms shall be supported.

5.6 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 TC 57 referencing standard requirements

Other standards referencing this technical specification shall specify:

– the mandatory Cipher Suites to be supported;

– the recommended time period in which encryption keys are to be exchanged;

– the recommended specification in regards to the re-negotiation of keys based upon protocol traffic. This shall specify the mechanism to measure the traffic (e.g. packets sent, bytes sent, etc.) and the recommended metric upon which re-negotiation should be performed;

– the recommended number of CAs to be supported;