IEC 62351-3

Edition 1.0 2014-10

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

IEC 62351-3:2014-10(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

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

IEC publications search - 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 It also gives information on projects, replaced and withdrawn publications.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
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 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
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
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: 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
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
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 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
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
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62351-3

Edition 1.0 2014-10

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

PRICE CODE
CODE PRIX

N

ICS 33.200

ISBN 978-2-8322-1900-3

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 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.

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*[1]

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*[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 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

---

1 Under consideration.

2 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.

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.

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

NOTE The option to remotely 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.

The refusal of a connection due to a expired certificate should raise a security event ("warning: 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.

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.

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.

5.6.4.7 Key exchange

Public key mechanisms 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 key length of 1 024 Bit (legacy mode);

– Mandatory: Recommended key length of at least 2 048 Bit (modern mode).

The optional support for 1 024 bit key length is intended for backward compatibility. 2 048 bit key length must be supported and is the preferred key length to be used.

1 024 bit 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 1 024 bits cannot be used, it is also recommended to take additional security measures. The usage of 1 024 bit key length 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.

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.

– The recommended time period in which encryption keys are to be exchanged (session key update).

– The recommended specification in regards to resumption of keys 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.

– The recommended specification in regards to the renegotiation of keys 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 certificate size.

– The recommended default CRL evaluation period.

– In case of using OCSP for certificate revocation checks, the handling of failures to access the OCSP responder.

– The handling of certificate revocation actions with respect to certificates used in the context of TLS. Revoking 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.

Bibliography

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

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

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*

SOMMAIRE

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.

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 norme annule et remplace l'IEC TS 62351-2:2007.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
57/1498/FDIS	57/1515/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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 cette publication 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.

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 TS 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management*[1] (disponible en anglais seulement)

ISO/IEC 9594-8, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: 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.

3.2 Autres abréviations

CRL Liste de révocation de certificat (*Certificate Revocation List*)

DER Règles de codage identifiées (*Distinguished Encoding Rules*)

ECDSA Algorithme de signature numérique de courbe elliptique (*Elliptic Curve Digital Signature Algorithm*)

---

[1] A l'étude.

[2] Généralement appelé SSL/TLS.

ECGDSA Algorithme de signature numérique allemand de courbe elliptique (*Elliptic Curve German Digital Signature Algorithm*) (voir l'ISO/IEC 15946-2)

OCSP Protocole de vérification en ligne de certificat (*Online Certificate Status Protocol*) (voir la RFC 6960)

PIXIT Informations complémentaires de mise en œuvre du protocole pour les essais (*Protocol Implementation eXtra Information for Testing*)

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). La présente partie de l'IEC 62351 ne couvre pas la sécurité pour les couches application de communication (couches OSI 5 et supérieures) ou la sécurité d'application à application.

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 spécifié 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.

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

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 liste des suites déconseillées comprend les suites suivantes, sans toutefois s'y limiter:

– TLS_NULL_WITH_NULL_NULL
– TLS_RSA_NULL_WITH_NULL_MD5

5.2 Négociation des versions

La TLS v1.2 telle que définie dans la RFC 5246 (parfois appelée SSL v3.3) ou version supérieure doit être prise en charge. Pour garantir la rétrocompatibilité, les mises en œuvre doivent aussi 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).

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.

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

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 l'impact sur les performances des protocoles de transfert asymétriques et 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 heures). La présente spécification adopte cette méthode. Il convient d'effectuer une reprise de session en moins de 24 heures, 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.

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/octets envoyés. Ces contraintes de temps/octets maximaux de reprise sont censées être spécifiées dans des PIXIT 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.

La reprise de session peut être initiée par l'un ou l'autre côté, tant que 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.

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 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/octets envoyés. Ces contraintes de temps/octets maximaux de renégociation sont censées être spécifiées dans des PIXIT (informations complémentaires de mise en œuvre du protocole pour les essais, *Protocol Implementation eXtra Information for Testing*) de la norme de référence.

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 effectuée au moins toutes les 24 heures 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.

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.

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.

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».

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 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.

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.

5.6.3 Échange de certificat

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

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.

NOTE 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.

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).

5.6.4.4 Révocation de certificat

La révocation de certificat doit être effectuée comme spécifié 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 d'une session. Une entité recevant un certificat révoqué au cours de l'établissement de la session doit refuser la connexion.

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.

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.

NOTE 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.

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.

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.

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.

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.

5.6.4.7 Échange de clés

Les mécanismes de clés publiques 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 minimale de 1 024 Bits (mode hérité);
– Obligatoire: Longueur de clé recommandée d'au moins 2 048 Bits (mode moderne).

La prise en charge facultative d'une longueur de clé 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.

Une longueur de clé 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 utilisation de 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.

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.

– 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 reprise des clés 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.

– La spécification recommandée concernant la renégociation des clés 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 certificat.

– La période par défaut recommandée d'évaluation de la CRL.

– Dans le cas où 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 de certificat par rapport aux certificats utilisés dans le contexte de la TLS. La révocation 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 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.

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 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)

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)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch