BS EN 62351-3:2014

BSI Standards Publication

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

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62351-3:2014. It is identical to IEC 62351-3:2014. It supersedes DD IEC/TS 62351-3:2007 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015.

ISBN 978 0 580 82842 3

ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62351-3

December 2014

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP
(IEC 62351-3:2014)

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
(CEI 62351-3:2014)

Management von Systemen der Energietechnik und zugehöriger Datenaustausch - Daten- und Kommunikationssicherheit - Teil 3: Sicherheit von Kommunikationsnetzen und Systemen - Profile einschließlich TCP/IP
(IEC 62351-3:2014)

This European Standard was approved by CENELEC on 2014-12-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62351-3:2014 E

Foreword

The text of document 57/1498/FDIS, future edition 1 of IEC 62351-3, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62351-3:2014.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2015-09-02
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2017-12-02

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62351-3:2014 was approved by CENELEC as a European Standard without any modification.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
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	- [1)]	Power systems management and associated information exchange - Data and communications security - Part 9: Key management	-	-
ISO/IEC 9594-8	-	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
RFC 4492	2006	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)	-	-
RFC 5246	2008	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
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	2011 [2)]	Transport Layer Security (TLS) Extensions: Extension Definitions	-	-
RFC 6176	2011	Prohibiting Secure Sockets Layer (SSL) Version 2.0	-	-

[1)] At draft stage.

[2)] Supersedes RFC 4366:2006, *Transport Layer Security (TLS) Extensions*.

CONTENTS

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*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™