SVENSK STANDARD SS-EN 62351-3

Fastställd	Utgåva	Sida	Ansvarig kommitté
2015-05-13	1	1 (1+16)	SEK TK 57

Styrning av kraftsystem och tillhörande informationsutbyte – IT-säkerhet – Del 3: Specifikation av säkerhet i kommunikationsnät baserade på TCP/IP

Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP

Som svensk standard gäller europastandarden EN 62351-3:2014. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62351-3:2014.

Nationellt förord

Europastandarden EN 62351-3:2014

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC

– **IEC 62351-3, First edition, 2014 - Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 33.200.00

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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

SEK Svensk Elstandard

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

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*

---

1 Under consideration.

2 This is typically referred to as SSL/TLS.