SVENSK STANDARD SS-EN 62351-9

Fastställd	Utgåva	Sida	Ansvarig kommitté
2018-02-21	1	1 (1+87)	SEK TK 57

Styrning av kraftsystem och tillhörande informationsutbyte – IT-säkerhet – Del 9: Cyber-säkerhetsrelaterad nyckelhantering

Power systems management and associated information exchange –
Data and communications security –
Part 9: Cyber security key management for power system equipment

Som svensk standard gäller europastandarden EN 62351-9:2017. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62351-9:2017.

Nationellt förord

Europastandarden EN 62351-9:2017

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC

– **IEC 62351-9, First edition, 2017 - Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment**

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 62351-9

July 2017

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9 :2017)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance
(IEC 62351-9 :2017)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 9: Cyber security Schlüssel-Management für Stromversorgungsanlagen
(IEC 62351-9 :2017)

This European Standard was approved by CENELEC on 2017-06-22. 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

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

European foreword

The text of document 57/1838/FDIS, future edition 1 of IEC 62351-9, 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 62351-9:2017.

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) 2018-03-22
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2020-06-22

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

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62351-9:2017 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62351-3	NOTE	Harmonized as EN 62351-3.

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 62351-2	-	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
ISO/IEC 9594-8/ Rec. ITU-T X.509	2017 2016	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
ISO/IEC 9834-1/ Rec. ITU-T X.660	2012 2011	Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree	-	-
RFC 5246	-	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
RFC 5272	-	Certificate Management over CMS (CMC)	-	-
RFC 5934	-	Trust Anchor Management Protocol (TAMP)	-	-
RFC 6407	-	The Group Domain of Interpretation	-	-
IETF RFC 6960	-	X.509 - Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	-	-
RFC 7030	-	Enrolment over Secure Transport	-	-

SCEP IETF Draft, Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 9: Cyber security key management for power system equipment

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 62351-9 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
57/1838/FDIS	57/1853/RVD

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

This document 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.

In this standard, the following print types are used:

– ASN.1 notions is presented in bold Courier New typeface;

– when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in bold Courier New typeface.

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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

Part 9: Cyber security key management for power system equipment

1 Scope

This part of IEC 62351 specifies cryptographic key management, namely how to generate, distribute, revoke, and handle public-key certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g. private keys and public-key certificates), as well as symmetric keys for groups (GDOI).

This part of IEC 62351 assumes that other standards have already chosen the type of keys and cryptography that will be utilized, since the cryptography algorithms and key materials chosen will be typically mandated by an organization’s own local security policies and by the need to be compliant with other international standards. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. The objective is to define requirements and technologies to achieve interoperability of key management.

The purpose of this part of IEC 62351 is to guarantee interoperability among different vendors by specifying or limiting key management options to be used. This document assumes that the reader understands cryptography and PKI principles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*

SCEP IETF Draft, *Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5272, *Certificate Management over CMS (CMC)*

RFC 5934, *Trust Anchor Management Protocol (TAMP)*

RFC 6407, *The Group Domain of Interpretation*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

RFC 7030, *Enrolment over Secure Transport*