IEC 62351-9

Edition 1.0 2017-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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 62351-9:2017-05(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 It also gives information on projects, replaced and withdrawn publications.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 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 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 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 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 62351-9

Edition 1.0 2017-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-5199-7

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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.

This bilingual version (2018-07) corresponds to the monolingual English version, published in 2017-05.

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.

The French version of this standard has not been voted upon.

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.

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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
asymmetric keys
two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification

3.2
authorization and validation list
AVL
signed list containing information to an AVL entity about potential communications entities and possible restrictions on the communications with such entities

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.9]

3.3
authorization and validation list entity
AVL entity
entity, when acting as a relying party, which is dependent on an AVL issued by a designated authorizer

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.10]

3.4
authorizer
entity trusted by one or more entities operating as AVL entities to create, maintain and sign authorization and validation lists

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.11]

3.5
certification path
ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the end-entity public-key certificate to be validated

Note 1 to entry: All intermediate public-key certificates, if any, are CA certificates in which the subject of the preceding public-key certificate is the issuer of the following public-key certificate.

[SOURCE: ISO/IEC 9594-8:2017, 3.5.18 | Rec. ITU-T X.509 (2016), 3.5.21]

3.6
certificate signing request
CSR
request issued when a new certificate or renewal of a certificate is required

Note 1 to entry: When the generated CSR is submitted to a CA, the CA signs the CSR using its private key and the CSR becomes the certificate.

Note 2 to entry: This note applies to the French language only.

[SOURCE: RFC 2986]

3.7
controllership
intersection of legal ownership, physical control, and logical control over a device or system, in which the nature of any contractual agreements between ownership and control of the device or system is not important in the context

3.8
cryptographic binding
use of one or more cryptographic techniques by a CKMS to establish a trusted association between a key and selected metadata elements

[SOURCE: NIST SP 800-130]

3.9
cryptographic key management system
CKMS
system for the management (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction) of cryptographic keys and their metadata

Note 1 to entry: This note applies to the French language only.

[SOURCE: NIST SP 800-130]

3.10
dataset
collection of data

3.11
digital signature
result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation

[SOURCE: FIPS 186]

3.12
entity
generic term that covers human users, automation systems, software applications, communication nodes, field devices, and other types of assets

3.13
group controller/key server
GCKS
device that defines group policy and distributes keys for that policy

Note 1 to entry: This note applies to the French language only.

[SOURCE: RFC 3740]

3.14
group domain of interpretation
GDOI
domain that manages group security associations, which are used by IPsec and potentially other data security protocols

Note 1 to entry: These security associations protect one or more key-encrypting keys (KEK), traffic-encrypting keys (TEK), or data shared by group members. GDOI uses the notion of a group controller, which is used to support the establishment of security associations between members of a group.

Note 2 to entry: This note applies to the French language only.

[SOURCE: RFC 6407]

3.15
group member
GM
authorized member of a secure group, sending and/or receiving IP packets related to the group

Note 1 to entry: This note applies to the French language only.

3.16
hash function
(mathematical) function which maps data of arbitrary size into data of a fixed size called a digest

Note 1 to entry: Approved hash functions satisfy the following properties:

1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output.

2) Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.

[SOURCE: ISO/IEC 9598-8:2017 | Rec. ITU-T X.509 (2016), 3.5.36]

3.17
hash message authentication code
HMAC
cryptographic code used for authentication with symmetric keys and for data integrity

Note 1 to entry: This note applies to the French language only.

[SOURCE: RFC 2104]

3.18
key distribution centre
KDC
centre which, in an IEC 62351-9 context, provides a network service that supplies temporary (symmetrical) session keys to predefined set of peers after successful authentication

Note 1 to entry: This is also known as Group Controller/Key Server (GCKS) (See GDOI).

Note 2 to entry: This note applies to the French language only.

3.19
message authentication code
MAC
cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modification of the data

Note 1 to entry: This note applies to the French language only.

[SOURCE: SP 800-63; FIPS 201]

3.20
object identifier
ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node

[SOURCE: ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), 3.5.11]

3.21
online certificate status protocol
OCSP
protocol that enables applications to determine the (revocation) state of an identified certificate

Note 1 to entry: OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

Note 2 to entry: This note applies to the French language only.

[SOURCE: RFC 6960]

3.22
pre-shared key
PSK
secret which is shared in advanced between the two entities, such as software applications or devices, to be able to authenticate themselves after establishing a secure connection

Note 1 to entry: This note applies to the French language only.

3.23
private key
(in a public-key cryptosystem) that key of an entity's key pair which is known only by that entity

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.49]

3.24
public-key certificate
public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it

Note 1 to entry: A public-key certificate is often called an X.509 certificate or a digital certificate. However, such terms are ambiguous, as they could also mean attribute certificates, which are also defined by ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.57]

3.25
public-key cryptography standards
PKCS
specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography

Note 1 to entry: This note applies to the French language only.

[SOURCE: www.rsa.com]

3.26
random number generation
RNG
process used to generate an unpredictable series of numbers

Note 1 to entry: Each individual value is called random if each of the values in the total population of values has an equal probability of being selected.

Note 2 to entry: This note applies to the French language only.

[SOURCE: NIST SP 800-57]

3.27
registration authority
those aspects of the responsibilities of a certification authority that are related to identification and authentication of the subject of a public-key certificate to be issued by that certification authority

Note 1 to entry: A registration authority may either be a separate entity or be an integrated part of the certification authority.

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T Rec. X.509 (2016), 3.5.60]

3.28
relying party
entity that relies on the data in a public-key certificate in making decisions

[SOURCE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.61]

3.29
secret key
cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public

[SOURCE: FIPS 140-2]

3.30
security association
SA
relationship established between two or more entities to enable them to protect data they exchange

Note 1 to entry: This note applies to the French language only.

[SOURCE: NIST IR 7298 Rev.1]

3.31
security strength
ability of the security technologies to make it infeasible for a would-be attacker to bypass or subvert

Note 1 to entry: This is often measured in bits of security.

[SOURCE: NIST SP 800-130]

3.32
session key
in the context of symmetric encryption, key that is temporary or is used for a relatively short period of time