

INTERNATIONAL STANDARD



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2017 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, replaced and withdrawn publications.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.

INTERNATIONAL STANDARD



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-4220-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviations and acronyms.....	14
5 Cryptographic applications for power system implementations.....	15
5.1 Cryptography, cryptographic keys, and security objectives.....	15
5.2 Types of cryptography	16
5.3 Uses of cryptography.....	16
5.3.1 Goals of cyber security	16
5.3.2 Confidentiality.....	17
5.3.3 Data integrity	17
5.3.4 Authentication.....	18
5.3.5 Non-repudiation.....	18
5.3.6 Trust.....	18
6 Key management concepts and methods in power system operations	19
6.1 Key management system security policy	19
6.2 Key management design principles for power system operations	19
6.3 Use of Transport Layer Security (TLS)	19
6.4 Cryptographic key usages.....	19
6.5 Trust using a public-key infrastructure (PKI).....	20
6.5.1 Registration authorities (RA).....	20
6.5.2 Certification authority (CA)	20
6.5.3 Public-key certificates.....	20
6.5.4 Attribute certificates.....	21
6.5.5 Public-key certificate and attribute certificate extensions	21
6.6 Trust via non-PKI self-signed certificates	22
6.7 Authorization and validation lists.....	22
6.7.1 General	22
6.7.2 AVLs in non-constrained environments	23
6.7.3 AVLs in constrained environments	23
6.7.4 Use of self-signed public-key certificates in AVLs	23
6.8 Trust via pre-shared keys.....	23
6.9 Session keys	24
6.10 Protocols used in trust establishment.....	24
6.10.1 Certification request	24
6.10.2 Trust Anchor Management Protocol (TAMP)	24
6.10.3 Simple Certificate Enrolment Protocol (SCEP)	24
6.10.4 Internet X.509 PKI Certificate Management Protocol (CMP).....	24
6.10.5 Certificate Management over CMS (CMC)	25
6.10.6 Enrolment over Secure Transport (EST)	25
6.10.7 Summary view on the different protocols	25
6.11 Group keys	26
6.11.1 Purpose of group keys.....	26
6.11.2 Group Domain of Interpretation (GDOI)	26
6.12 Key management lifecycle	31

6.12.1	Key management in the life cycle of an entity	31
6.12.2	Cryptographic key lifecycle	32
6.13	Certificate management processes	34
6.13.1	Certificate management process	34
6.13.2	Initial certificate creation	34
6.13.3	Enrolment of an entity	34
6.13.4	Certificate signing request (CSR) process	36
6.13.5	Certificate revocation lists (CRLs)	37
6.13.6	Online certificate status protocol (OCSP)	38
6.13.7	Server-based certificate validation protocol (SCVP)	41
6.13.8	Short-lived certificates	41
6.13.9	Certificate renewal	42
6.14	Alternative process for asymmetric keys generated outside the entity	43
6.15	Key distribution for symmetric keys with different time frames	44
7	General key management requirements	44
7.1	Asymmetric and symmetric key management requirements	44
7.2	Required cryptographic materials	44
7.3	Public-Key certificates requirements	45
7.4	Cryptographic key protection	45
7.5	Use of existing security key management infrastructure	45
7.6	Use of object identifiers	45
8	Asymmetric key management	45
8.1	Certificate generation and installation	45
8.1.1	Private and public key generation and installation	45
8.1.2	Private and public key renewal	46
8.1.3	Random Number Generation	46
8.1.4	Certificate policy	46
8.1.5	Entity registration for identity establishment	46
8.1.6	Entity configuration	47
8.1.7	Entity enrolment	47
8.1.8	Trust anchor information update	48
8.2	Public-key certificate revocation	49
8.3	Certificate validity	49
8.3.1	Validity of certificates	49
8.3.2	Certificate revocation	50
8.3.3	Certificate revocation status checking	50
8.3.4	Handling of authorization and validation lists (AVLs)	50
8.4	Certificate expiration and renewal	55
8.5	Secured Time Synchronization	55
9	Symmetric key management	56
9.1	Group based key management (GDOI)	56
9.1.1	GDOI requirements	56
9.1.2	Internet Key Exchange Version 1 (IKEv1)	56
9.1.3	Phase 1 IKEv1 main mode exchange type 2	57
9.1.4	Phase 1/2 ISAKMP informational exchange type 5	60
9.1.5	Phase 2 GDOI GROUPKEY-PULL exchange type 32	62
9.1.6	GROUPKEY-PULL group key download exchange	70
10	Connections to the IEC 62351 parts and other IEC documents	71

Annex A (normative) Protocol Implementation Conformance Statement (PICS).....	73
Annex B (informative) Random Number Generation (RNG)	74
B.1 Random number generation types.....	74
B.2 Deterministic random bit generators.....	74
B.3 Non-deterministic random number generation	75
B.4 Entropy sources	75
Annex C (informative) Certificate enrolment and renewal flowcharts	76
C.1 Certificate enrolment.....	76
C.2 Certificate renewal.....	76
Annex D (informative) Examples of certificate profiles.....	78
Bibliography.....	82
Figure 1 – Relationship between public-key certificates and attribute certificates	21
Figure 2 – Group key management distribution	26
Figure 3 – GDOI IKE Phase 1 – Authentication and securing communication channel	27
Figure 4 – GDOI Pull Phase 2.....	28
Figure 5 – Key renewal triggered by the entities.....	30
Figure 6 – Key management in product life cycle	31
Figure 7 – Simplified certificate life cycle	32
Figure 8 – Cryptographic key life cycle	33
Figure 9 – Example of the SCEP entity enrolment and CSR process.....	35
Figure 10 – Example of the EST entity enrolment and CSR process	36
Figure 11 – CSR processing	37
Figure 12 – Certificate revocation list.....	38
Figure 13 – Overview of the online certificate status protocol (OCSP).....	39
Figure 14 – Diagram using a combination of CRL and OCSP processes	40
Figure 15 – Call Flows for the Online Certificate Status Protocol (OCSP).....	41
Figure 16 – Overview Server-Based Certificate Validation Protocol using OCSP Backend	41
Figure 17 – SCEP certificate renewal.....	42
Figure 18 – EST certificate renewal/rekeying	43
Figure 19 – Central certificate generation	44
Figure 20 – IKEv1 (RFC 2409) main mode exchange with RSA digital signatures	57
Figure 21 – IKEv1 main mode exchange and security association messages	58
Figure 22 – IKEv1 main mode exchange: key exchange messages	59
Figure 23 – IKEv1 Main Mode Exchange: ID authentication messages.....	59
Figure 24 – IKEv1 HASH_I calculation	60
Figure 25 – Phase 1 Informational Exchange	61
Figure 26 – GD004FI GROUPKEY-PULL as define in RFC 6407	62
Figure 27 – GROUPKEY-PULL hash computations	63
Figure 28 – GROUPKEY-PULL initial SA request exchange	64
Figure 29 – RFC 6407 Identification Payload	64
Figure 30 – ID_OID Identification Data.....	65
Figure 31 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF	66

Figure 32 – IPADDRESS ASN.1 BNF	66
Figure 33 – Example IecUdpAddrPayload ASN.1 Data with DER Encoding	67
Figure 34 – 61850_UDP_TUNNEL Payload ASN.1 BNF	67
Figure 35 – 61850_ETHERNET_GOOSE/SV Payload ASN.1 BNF	67
Figure 36 – RFC 6407 SA TEK Payload	68
Figure 37 – IEC-61850 SA TEK Payload	69
Figure 38 – GROUPKEY-PULL Key Download Exchange	70
Figure 39 – IEC 62351 Part 9 relationship to other IEC 62351 parts	71
Figure C.1 – Certificate enrolment	76
Figure C.2 – Certificate renewal state machine	77
Table 1 – KDC IKEv1 Requirements	56
Table 2 – IEC 61850 Object IDs: Mandatory (m) and Optional (o)	65
Table D.1 – Examples of operator public-key certificates	79
Table D.2 – Examples of OEM certificates	80
Table D.3 – Example of OCSP certificate	81

a preview generated by EVS

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*

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]