

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 62351-9:2017 sisaldab Euroopa standardi EN 62351-9:2017 ingliskeelset teksti.	This Estonian standard EVS-EN 62351-9:2017 consists of the English text of the European standard EN 62351-9:2017.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 07.07.2017.	Date of Availability of the European standard is 07.07.2017.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 33.200

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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.



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

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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

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

This document is a preview generated by EVS

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*