

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



---

**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

CONTENTS .....	2
FOREWORD .....	6
1 Scope .....	8
2 Normative references .....	8
3 Terms and definitions .....	9
4 Abbreviations and acronyms .....	15
5 Cryptographic applications for power system implementations .....	16
5.1 Cryptography, cryptographic keys, and security objectives .....	16
5.2 Types of cryptography .....	16
5.3 Uses of cryptography .....	17
5.3.1 Goals of cyber security .....	17
5.3.2 Confidentiality .....	18
5.3.3 Data integrity .....	18
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) .....	20
6.4 Cryptographic key usages .....	20
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 .....	21
6.5.4 Attribute certificates .....	21
6.5.5 Public-key certificate and attribute certificate extensions .....	22
6.6 Trust via non-PKI self-signed certificates .....	22
6.7 Authorization and validation lists .....	23
6.7.1 General .....	23
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 .....	24
6.8 Trust via pre-shared keys .....	24
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) .....	25
6.10.3 Simple Certificate Enrolment Protocol (SCEP) .....	25
6.10.4 Internet X.509 PKI Certificate Management Protocol (CMP) .....	25
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 .....	26
6.11 Group keys .....	26
6.11.1 Purpose of group keys .....	26
6.11.2 Group Domain of Interpretation (GDOI) .....	27

- 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 .....	22
Figure 2 – Group key management distribution .....	27
Figure 3 – GDOI IKE Phase 1 – Authentication and securing communication channel.....	28
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

## 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*

## SOMMAIRE

AVANT-PROPOS .....	90
1 Domaine d'application .....	92
2 Références normatives .....	92
3 Termes et définitions .....	93
4 Abréviations et acronymes.....	99
5 Applications cryptographiques pour les mises en œuvre de systèmes de puissance .....	100
5.1 Cryptographie, clés cryptographiques et objectifs de sécurité .....	100
5.2 Types de cryptographies .....	101
5.3 Utilisations de la cryptographie .....	102
5.3.1 Objectifs de la cybersécurité.....	102
5.3.2 Confidentialité .....	102
5.3.3 Intégrité des données .....	102
5.3.4 Authentification.....	103
5.3.5 Non-répudiation .....	103
5.3.6 Confiance .....	103
6 Concepts et méthodes de gestion de clé dans les opérations du système de puissance .....	104
6.1 Politique de sécurité du système de gestion de clé .....	104
6.2 Principes de conception de la gestion de clé pour les opérations du système de puissance .....	104
6.3 Utilisation de la Sécurité de la couche transport (TLS).....	105
6.4 Utilisations de clés cryptographiques .....	105
6.5 Confiance à l'aide d'une infrastructure à clés publiques (PKI) .....	105
6.5.1 Autorités d'enregistrement (RA).....	105
6.5.2 Autorité de certification (AC).....	106
6.5.3 Certificats de clé publique .....	106
6.5.4 Certificats d'attribut .....	106
6.5.5 Extensions de certificat de clé publique et de certificat d'attribut.....	108
6.6 Confiance via les certificats autosignés non PKI .....	108
6.7 Listes d'autorisation et de validation .....	109
6.7.1 Généralités .....	109
6.7.2 AVL dans les environnements non restreints .....	109
6.7.3 AVL dans les environnements restreints .....	109
6.7.4 Utilisation de certificats autosignés de clé publique dans les AVL.....	110
6.8 Confiance via les clés prépartagées.....	110
6.9 Clés de session .....	110
6.10 Protocoles utilisés dans l'établissement de confiance .....	110
6.10.1 Demande de certification .....	110
6.10.2 Protocole de gestion des ancres de confiance (TAMP) .....	111
6.10.3 Protocole simple d'enregistrement de certificat (SCEP) .....	111
6.10.4 Protocole de gestion de certificats (CMP – <i>certificate management protocol</i> ) PKI Internet X.509.....	111
6.10.5 Gestion de certificats sur CMS (CMC) .....	111
6.10.6 Enregistrement sur transport sécurisé (EST – <i>enrolment over secure transport</i> ).....	112
6.10.7 Récapitulatif des différents protocoles .....	112

6.11	Clés de groupe .....	112
6.11.1	Objet des clés de groupe .....	112
6.11.2	Domaine d'interprétation de groupe (GDOI) .....	113
6.12	Cycle de vie de la gestion de clé.....	119
6.12.1	Gestion de clé dans le cycle de vie d'une entité .....	119
6.12.2	Cycle de vie d'une clé cryptographique .....	123
6.13	Processus de gestion de certificats .....	125
6.13.1	Processus de gestion de certificats.....	125
6.13.2	Création de certificat initial .....	125
6.13.3	Enregistrement d'une entité .....	125
6.13.4	Processus de demande de signature de certificat (CSR).....	129
6.13.5	Listes de révocation de certificat (CRL – <i>certificate revocation list</i> ).....	130
6.13.6	Protocole de vérification en ligne de certificat (OCSP).....	131
6.13.7	Protocole SCVP ( <i>Server-based Certificate Validation Protocol</i> – Protocole de validation des certificats basé sur serveur).....	135
6.13.8	Certificats éphémères .....	136
6.13.9	Renouvellement de certificat.....	136
6.14	Processus alternatif pour les clés asymétriques générées hors de l'entité .....	139
6.15	Distribution de clés symétriques avec des intervalles de temps différents .....	140
7	Exigences relatives à la gestion générale de clés .....	141
7.1	Exigences relatives à la gestion de clé asymétrique et symétrique .....	141
7.2	Composants cryptographiques exigés .....	141
7.3	Exigences relatives aux certificats de clé publique .....	141
7.4	Protection de clé cryptographique .....	141
7.5	Utilisation de l'infrastructure de gestion de clé de sécurité existante .....	141
7.6	Utilisation des identificateurs d'objet .....	141
8	Gestion de clé asymétrique .....	142
8.1	Génération et installation de certificat .....	142
8.1.1	Génération et installation de clé privée et de clé publique.....	142
8.1.2	Renouvellement de clé privée et de clé publique .....	142
8.1.3	Génération de nombres aléatoires .....	142
8.1.4	Politique de certification .....	142
8.1.5	Enregistrement d'entité pour l'établissement d'identité .....	143
8.1.6	Configuration d'entité.....	143
8.1.7	Enregistrement d'entité.....	143
8.1.8	Mise à jour des informations d'ancre de confiance .....	145
8.2	Révocation de certificat de clé publique .....	146
8.3	Validité de certificat .....	146
8.3.1	Validité des certificats.....	146
8.3.2	Révocation de certificat .....	147
8.3.3	Vérification de l'état de révocation d'un certificat .....	147
8.3.4	Gestion des listes d'autorisation et de validation (AVL).....	147
8.4	Expiration et renouvellement de certificat.....	152
8.5	Synchronisation temporelle sécurisée .....	153
9	Gestion de clé symétrique .....	153
9.1	Gestion de clé basée sur les groupes (GDOI) .....	153
9.1.1	Exigences GDOI .....	153
9.1.2	Internet Key Exchange Version 1 (IKEv1) .....	153
9.1.3	Mode principal IKEv1 Phase 1, type d'échange 2.....	154

9.1.4	Échange informationnel ISAKMP Phase 1/2, type d'échange 5 .....	159
9.1.5	Type d'échange 32 GROUPKEY-PULL GDOI de phase 2 .....	161
9.1.6	Échange Téléchargement de clé de groupe GROUPKEY-PULL .....	170
10	Correspondances entre les parties de l'IEC 62351 et d'autres documents de l'IEC .....	171
Annexe A (normative) Déclarations de conformité de mise en œuvre du protocole (PICS).....		174
Annexe B (informative) Génération de nombres aléatoires (RNG).....		175
B.1	Types de générations de nombres aléatoires .....	175
B.2	Générateurs de bits aléatoires déterministes .....	175
B.3	Génération de nombres aléatoires non déterministes .....	176
B.4	Sources d'entropie .....	177
Annexe C (informative) Diagrammes d'enregistrement et de renouvellement de certificat .....		178
C.1	Enregistrement de certificat .....	178
C.2	Renouvellement de certificat .....	179
Annexe D (informative) Exemples de profils de certificat.....		181
Bibliographie.....		188
Figure 1 – Relation entre les certificats de clé publique et les certificats d'attribut .....		107
Figure 2 – Distribution de la gestion de clé de groupe.....		113
Figure 3 – Échange de clé Internet GDOI – Phase 1 – Authentification et sécurisation de la voie de communication.....		114
Figure 4 – Pull de GDOI – Phase 2 .....		115
Figure 5 – Renouvellement de clé déclenché par les entités .....		118
Figure 6 – Gestion de clé dans le cycle de vie du produit.....		120
Figure 7 – Cycle de vie simplifié d'un certificat.....		123
Figure 8 – Cycle de vie d'une clé cryptographique .....		123
Figure 9 – Exemple d'enregistrement de l'entité SCEP et processus de demande de signature de certificat (CSR).....		126
Figure 10 – Exemple d'enregistrement de l'entité EST et processus de demande de signature de certificat (CSR).....		128
Figure 11 – Traitement d'une demande de signature de certificat.....		130
Figure 12 – Liste de révocation de certificat.....		131
Figure 13 – Présentation du protocole de vérification en ligne de certificat (OCSP) .....		132
Figure 14 – Schéma utilisant une combinaison de CRL et de processus OCSP.....		134
Figure 15 – Flux d'appel du protocole de vérification en ligne de certificat (OCSP) .....		135
Figure 16 – Présentation du protocole SCVP à l'aide du système principal OCSP.....		136
Figure 17 – Renouvellement de certificat SCEP .....		137
Figure 18 – Renouvellement de certificat EST/de clé .....		139
Figure 19 – Génération centrale de certificat.....		140
Figure 20 – Échange IKEv1 en mode principal (RFC 2409) avec des signatures numériques RSA.....		155
Figure 21 – Échange IKEv1 en mode principal et messages d'association de sécurité .....		156
Figure 22 – Échange IKEv1 en mode principal: messages d'échange de clé .....		157
Figure 23 – Échange IKEv1 en mode principal: messages d'authentification d'ID .....		158
Figure 24 – Calcul d'IKEv1 HASH_I .....		158

Figure 25 – Échange informationnel de phase 1.....	159
Figure 26 – Échange GROUPKEY-PULL GDOI tel que défini dans le RFC 6407 .....	161
Figure 27 – Calculs de hachage GROUPKEY-PULL.....	162
Figure 28 – Échange Demande d'association de sécurité initiale GROUPKEY-PULL .....	163
Figure 29 – Charge utile Identification (RFC 6407) .....	163
Figure 30 – Données d'identification ID_OID.....	164
Figure 31 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF .....	165
Figure 32 – IPADDRESS ASN.1 BNF.....	166
Figure 33 – Exemple de données ASN.1 IecUdpAddrPayload avec codage DER .....	166
Figure 34 – Charge utile 61850_UDP_TUNNEL ASN.1 BNF .....	167
Figure 35 – Charge utile 61850_ETHERNET_GOOSE/SV ASN.1 BNF.....	167
Figure 36 – Charge utile SA TEK (RFC 6407) .....	168
Figure 37 – Charge utile SA TEK IEC-61850.....	169
Figure 38 – Échange Téléchargement de clé GROUPKEY-PULL .....	171
Figure 39 – Relation entre la Partie 9 de l'IEC 62351 et les autres parties de l'IEC 62351 .....	173
Figure C.1 – Enregistrement de certificat .....	179
Figure C.2 – Diagramme d'états de renouvellement de certificat.....	180
Tableau 1 – Exigences IKEv1 du centre de distribution de clé.....	154
Tableau 2 – ID d'objet IEC 61850: obligatoires (o) et facultatifs (f).....	165
Tableau D.1 – Exemples de certificats d'opérateur à clé publique .....	182
Tableau D.2 – Exemples de certificats d'OEM.....	184
Tableau D.3 – Exemples de certificats d'OCSP .....	186

## COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

---

### **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**

##### AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62351-9 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

La présente version bilingue (2018-07) correspond à la version anglaise monolingue publiée en 2017-05.

Le texte anglais de cette norme est issu des documents 57/1838/FDIS et 57/1853/RVD.

Le rapport de vote 57/1853/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote. Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Dans la présente norme, les caractères d'imprimerie suivants sont utilisés:

- les notions ASN.1 sont présentées en caractères gras avec la police Courier New;
- lorsque les types et les valeurs de ASN.1 sont référencés dans le texte normal, ils sont différenciés du texte normal en étant présentés en caractères gras avec la police Courier New.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.**

# 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

### 1 Domaine d'application

La présente partie de l'IEC 62351 porte sur la gestion de clé cryptographique, c'est-à-dire sur la manière de générer, distribuer, révoquer et manipuler les certificats de clé publique et les clés cryptographiques pour protéger les données numériques et leurs communications. La manipulation des clés asymétriques (les clés privées et les certificats de clé publique, par exemple) et les clés symétriques pour les groupes (GDOI) font également partie du domaine d'application de la présente norme.

La présente partie de l'IEC 62351 part du principe que d'autres normes ont déjà choisi le type de clés et la cryptographie qui seront utilisés, dans la mesure où les algorithmes de cryptographie et les supports de clé choisis sont en principe liés aux politiques de sécurité locales propres à une organisation et à la nécessité de satisfaire aux autres normes internationales. Le présent document spécifie donc uniquement les techniques de gestion de ces infrastructures de clé et de cryptographie sélectionnées. Il s'agit de définir les exigences et les technologies permettant d'assurer l'interopérabilité de la gestion de clé.

La présente partie de l'IEC 62351 a pour objet de garantir l'interopérabilité entre les différents fournisseurs en spécifiant ou limitant les options de gestion de clé à utiliser. Le présent document part du principe que le lecteur comprend les principes de cryptographie et d'infrastructure à clés publiques.

### 2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

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

ISO/IEC 9834-1:2012 | Rec. UIT-T X.660 (2011), *Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationaux*

SCEP IETF Draft, *Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt* (disponible en anglais seulement)

RFC 5246, *Protocole Sécurité de la couche Transport (TLS) version 1.2*

RFC 5272, *Certificate Management over CMS (CMC)* (disponible en anglais seulement)



RFC 5934, *Trust Anchor Management Protocol (TAMP)* (disponible en anglais seulement)

RFC 6407, *Domaine d'interprétation de groupe*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*  
(disponible en anglais seulement)

RFC 7030, *Enrolment over Secure Transport* (disponible en anglais seulement)