IEC 62351-9

Edition 2.0 2023-06

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 978-2-8322-6950-3

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 8
1 Scope 10
2 Normative references 11
3 Terms, definitions, and abbreviations 12
3.1 Terms and definitions 12
3.2 Abbreviations and acronyms 17
4 Security concepts applicable to power systems 19
4.1 General 19
4.2 Security objectives 19
4.2.1 Confidentiality 19
4.2.2 Data integrity 19
4.2.3 Authentication 19
4.2.4 Non-repudiation 20
4.3 Cryptographic algorithms and concepts 20
5 Key establishment and management techniques 21
5.1 General 21
5.2 Key management lifecycle 21
5.2.1 Key management in the life cycle of a device 21
5.2.2 Lifecycle of a cryptographic key 23
5.3 Cryptographic key usages 24
5.4 Key management system security policy 25
5.5 Key management design principles for power system operations 25
5.6 Establishment of symmetric keys 26
5.6.1 Overview 26
5.6.2 The Diffie-Hellman key agreement method 26
5.6.3 Key derivation function (KDF) method 26
5.6.4 Group key management 27
5.7 Trust supported by public-key infrastructures (PKI) and privilege management infrastructures (PMI) 30
5.7.1 General 30
5.7.2 Registration authorities (RA) 30
5.7.3 Certification authority (CA) 30
5.7.4 Public-key certificates 31
5.7.5 Attribute certificates 32
5.7.6 Public-key certificate and attribute certificate extensions 33
5.8 Certificate management of public-key certificates 33
5.8.1 Certificate management process 33
5.8.2 Initial certificate creation 34
5.8.3 Onboarding of an entity 34
5.8.4 Enrolment of an entity 35
5.8.5 Certificate signing request (CSR) processing 38
5.8.6 Enrolment Protocols 41
5.8.7 Trust Anchor Management Protocol (TAMP) 42
5.9 Revocation of public-key certificates 42
5.9.1 Certificate revocation lists (CRLs) 42
5.9.2 Online certificate status protocol (OCSP) 43
5.9.3 Server-based certificate validation protocol (SCVP) 46

5.9.4 Recovering from certificate revocation of an end entity 47
5.10 Trust via non-PKI issued (self-signed) certificates 47
5.11 Authorization and validation lists 48
5.11.1 General 48
5.11.2 AVLs in non-constrained environments 48
5.11.3 AVLs in constrained environments 49
6 Key management (normative) 49
6.1 General 49
6.2 Handling of security events 49
6.3 Required cryptographic material 50
6.4 Random Number Generation 50
6.5 Object identifiers 50
6.5.1 Concept of object identifiers 50
6.5.2 Use of object identifiers by this document 50
7 Asymmetric key management (normative) 51
7.1 General 51
7.2 Certificate components 51
7.2.1 Public-Key certificate components 51
7.2.2 Attribute certificate components 52
7.3 Certificate generation and installation 53
7.3.1 Private and public key generation and installation 53
7.3.2 Cryptographic key protection 54
7.3.3 Use of existing security key management infrastructure 54
7.3.4 Certificate policy 54
7.3.5 Entity registration for identity establishment 55
7.3.6 Entity configuration 55
7.3.7 Entity enrolment 56
7.3.8 Trust anchor information update 58
7.4 Certificate components and certificate verification 58
7.4.1 General 58
7.4.2 Certificate format and encoding 58
7.4.3 Certificate signature verification 59
7.4.4 Public-key certificate components 59
7.4.5 Attribute certificate components 66
7.4.6 Certificate revocation status 69
7.5 Certificate revocation 70
7.6 Certificate expiration and renewal 71
7.7 Clock Synchronization and Accuracy 72
7.8 Authorization and validation lists 72
7.8.1 General 72
7.8.2 Syntax for authorization and validation list (AVL) for public-key certificates 72
7.8.3 AVL scope restriction 73
7.8.4 AVL protocol restriction extension 74
7.8.5 AVL pinning of certificate and associated identifier 74
7.8.6 Public-key certificate extensions related to use of AVLs 75
7.8.7 Issuing of an AVL 75
7.8.8 Endpoint Handling of AVLs 75
8 Group based key management (normative) 75

8.1 GDOI requirements 75
8.2 Internet Key Exchange Version 1 (IKEv1) 76
8.3 Phase 1 IKEv1 main mode exchange type 2 77
8.3.1 General 77
8.3.2 Certificate request payload 78
8.3.3 Security association exchange (1) 78
8.3.4 Key exchange (2) 79
8.3.5 ID authentication exchange (3) 80
8.4 Phase 1/2 ISAKMP informational exchange type 5 81
8.4.1 General 81
8.4.2 Phase 1 informational exchange 82
8.4.3 Phase 2 Informational Exchange 83
8.5 Phase 2 GDOI GROUPKEY-PULL exchange type 32 83
8.5.1 General 83
8.5.2 Hash computations 84
8.5.3 Multi-sender and counter mode encryption algorithm 85
8.5.4 SA KEK, SEQ, KEK/LKH key download payload support 85
8.5.5 GROUPKEY-PULL group SA request exchange 85
8.5.6 SA TEK payload 90
8.5.7 IEC 61850 SA TEK payload 91
8.5.8 SA TEK payload for IEC 61850-9-3 92
8.5.9 SPI discussion 94
8.5.10 SA data attributes 95
8.5.11 GROUPKEY-PULL group key download exchange 95
8.5.12 TEK Key Download Handling 98
8.6 Phase 2 GROUPKEY-PUSH exchange type 33 98
8.6.1 General 98
8.6.2 GROUPKEY-PUSH Message 99
8.6.3 GROUPKEY-PUSH acknowledgement message 99
8.7 Operational considerations 100
8.7.1 General 100
8.7.2 Group Security Policy 100
8.7.3 Group dynamicity 100
8.7.4 Handling of Key Delivery Assurance (informative) 102
9 Protocol Implementation Conformance Statement (PICS) 102
9.1 General 102
9.2 Notation 103
9.3 Conformance to general key management requirements 103
9.4 Conformance to requirements for asymmetric key management 103
9.5 Requirements for group-based key management 104
9.6 Supported GDOI Payload OIDs 104
Annex A (informative) Relations to other parts of IEC 62351 and other IEC documents 105
Annex B (informative) Cryptographic algorithms and mechanisms 107
B.1 Trust and trust anchor 107
B.2 Cryptographic algorithms 107
B.2.1 Introduction 107
B.2.2 Security strength 108
B.3 Public-key algorithms 108
B.3.1 General 108

B.3.2 The RSA public-key algorithm 109
B.3.3 The DSA public-key algorithm 110
B.3.4 The ECDSA public-key algorithm 110
B.3.5 The EdDSA public-key algorithms 112
B.3.6 Digital signature algorithms 114
B.4 Symmetric key algorithms 116
B.4.1 Stream ciphers vs. block ciphers 116
B.4.2 Advance encryption standard 116
B.4.3 Advanced encryption standard – cipher block chaining (AES-CBC) 117
B.4.4 Advanced encryption standard – counter mode (AES-CTR) 117
B.5 Hash algorithms 118
B.6 Integrity check value (ICV) algorithms 119
B.6.1 General 119
B.6.2 Keyed-hash message authentication code (HMAC) algorithm 119
B.6.3 Advance Encryption Standard (AES) – Galois message authentication code (GMAC) algorithm 120
B.7 Authenticated encryption with associated data (AEAD) algorithms 120
B.7.1 General 120
B.7.2 Advanced encryption standard (AES) – Galois/Counter Mode (GCM) 121
B.7.3 Advanced encryption standard (AES) – Counter with CBC-MAC (CCM) 121
B.8 Diffie-Hellman key agreement 122
B.8.1 General 122
B.8.2 Introduction to cyclic groups 122
B.8.3 Diffie-Hellman method over finite field 123
B.8.4 The discrete logarithm problem 123
B.8.5 Elliptic curve Diffie-Hellman key agreement 123
B.8.6 Key establishment algorithms 124
B.9 Key derivation 125
B.10 Migration of cryptographic algorithms 126
B.11 Post-quantum computing cryptography 126
B.12 Random Number Generation (RNG) 127
B.12.1 Random number generation types 127
B.12.2 Deterministic random bit generators 127
B.12.3 Non-deterministic random number generation 128
B.12.4 Entropy sources 128
Annex C (informative) Certificate enrolment and renewal flowcharts 129
C.1 Certificate Enrolment 129
C.2 Certificate Renewal 130
Annex D (informative) Security Event mapping to IEC 62351-14 131
D.1 General 131
D.2 Security event log records for credential transport and enrolment 131
D.3 Security event log records for public-key certificate verification 132
D.4 Security event log records for attribute certificate verification 134
D.5 Security event log records for certificate revocation status 136
D.6 Security event log records for group-based key management with GDOI 137
Bibliography 138

Figure 1 – Overview key management in the life cycle of an entity 22

Figure 2 – Cryptographic key life cycle 23
Figure 3 – Overview of group key management on the example of GDOI 27
Figure 4 – GDOI IKE Phase 1 – Authentication and securing communication channel 28
Figure 5 – GDOI Pull Phase 2 29
Figure 6 – Overview of PKI infrastructure and realization examples 30
Figure 7 – Central certificate generation 32
Figure 8 – Relationship between public-key certificates and attribute certificates 33
Figure 9 – Example of the SCEP entity enrolment and CSR process 36
Figure 10 – Example of the EST entity enrolment and CSR process 37
Figure 11 – CSR processing 38
Figure 12 – Certification request format 39
Figure 13 – Certificate request message format 40
Figure 14 – Certificate revocation list 43
Figure 15 – Overview of the online certificate status protocol (OCSP) 44
Figure 16 – Diagram using a combination of CRL and OCSP processes 45
Figure 17 – Call Flows for the Online Certificate Status Protocol (OCSP) 46
Figure 18 – Overview Server-Based Certificate Validation Protocol using OCSP Backend 47
Figure 19 – IKEv1 (RFC 2409) main mode exchange with RSA digital signatures 78
Figure 20 – IKEv1 main mode exchange and security association messages 78
Figure 21 – IKEv1 main mode exchange: key exchange messages 79
Figure 22 – IKEv1 Main Mode Exchange: ID authentication messages 80
Figure 23 – IKEv1 HASH_I calculation 81
Figure 24 – Phase 1 Informational Exchange (cf. RFC 2408, section 4.8) 82
Figure 25 – Phase 2 Informational Exchange (cf. RFC 2409, section 5.7) 83
Figure 26 – IKEv1 HASH(1) calculation 83
Figure 27 – GDOI GROUPKEY-PULL as defined in RFC 6407 84
Figure 28 – GROUPKEY-PULL hash computations 84
Figure 29 – GROUPKEY-PULL initial SA request exchange 85
Figure 30 – RFC 6407 Identification Payload 86
Figure 31 – ID_OID Identification Data 87
Figure 32 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF 88
Figure 33 – IPADDRESS ASN.1 BNF 88
Figure 34 – Example IecUdpAddrPayload ASN.1 Data with DER Encoding 89
Figure 35 – 61850_UDP_TUNNEL Payload ASN.1 BNF 89
Figure 36 – 61850_ETHERNET_GOOSE/SV Payload ASN.1 BNF 89
Figure 37 – RFC 6407 SA TEK Payload 90
Figure 38 – IEC-61850 SA TEK Payload 91
Figure 39 – Correlation of SPI Value 94
Figure 40 – GROUPKEY-PULL Key Download Exchange 95
Figure 41 – GROUPKEY-PULL group key download hash computations 95
Figure 42 – Key renewal triggered by the entities 97
Figure 43 – GROUPKEY-PUSH message (from RFC 6407) 98

Figure 44 – GROUPKEY-PUSH ACK message (from RFC 8263) 98
Figure 45 – GROUPKEY-PUSH ACK hash computations 99
Figure 46 – GROUPKEY-PUSH ack_key computations 99
Figure A.1 – IEC 62351-9 relationship to other parts of IEC 62351 105
Figure C.1 – Certificate Enrolment (general) 129
Figure C.2 – Certificate Renewal State Machine 130

Table 1 – Public-key certificate components 51
Table 2 – Attribute certificate components 53
Table 3 – KDC IKEv1 Requirements 76
Table 4 – IEC 61850 Object IDs: Mandatory (m) and Optional (o) 87
Table 5 – PICS for general key management 103
Table 6 – PICS for asymmetric key management 103
Table 7 – PICS for group-based key management (valid for KDC and Client) 104
Table 8 – PICS for supported OIDs for the identification payload 104
Table D.1 – Security event logs for credential transport and certificate enrolment mapped to IEC 62351-14 131
Table D.2 – Security event logs defined for public-key certificate verification mapped to IEC 62351-14 132
Table D.3 – Security event logs defined for attribute certificate verification mapped to IEC 62351-14 134
Table D.4 – Security event logs defined for certificate revocation status mapped to IEC 62351-14 136
Table D.5 – Security event logs for GDOI mapped to IEC 62351-14 137

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.

IEC 62351-9 has been prepared by WG15: Data and Communication Security, of IEC technical committee TC57: Power systems management and associated information exchange. It is an International Standard.

This second edition cancels and replaces the first edition published in 2017. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Certificate components and verification of the certificate components have been added;
b) GDOI has been updated to include findings from interop tests;
c) GDOI operation considerations have been added;
d) GDOI support for PTP (IEEE 1588) support has been added as specified by IEC/IEEE 61850-9-3 Power Profile;
e) Cyber security event logging has been added as well as the mapping to IEC 62351-14;

f) Annex B with background on utilized cryptographic algorithms and mechanisms has been added.

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

Draft	Report on voting
57/2579/FDIS	57/2594/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

Abstract Syntax Notation One (ASN.1): `in courier new` and **`bold courier new`** `type`.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under 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 document 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, primarily focused on the management of long-term keys, which are most often asymmetric key pairs, such as public-key certificates and corresponding private keys. As certificates build the base this document builds a foundation for many IEC 62351 services (see also Annex A). Symmetric key management is also considered but only with respect to session keys for group-based communication as applied in IEC 62351-6. The objective of this document is to define requirements and technologies to achieve interoperability of key management by specifying or limiting key management options to be used.

This document assumes that an organization (or group of organizations) has defined a security policy to select the type of keys and cryptographic algorithms that will be utilized, which may have to align with other standards or regulatory requirements. This document therefore specifies only the management techniques for these selected key and cryptography infrastructures. This document assumes that the reader has a basic understanding of cryptography and key management principles.

The requirements for the management of pairwise symmetric (session) keys in the context of communication protocols is specified in the parts of IEC 62351 utilizing or specifying pairwise communication such as:

- IEC 62351-3 for TLS by profiling the TLS options
- IEC 62351-4 for the application layer end-to-end security
- IEC TS 62351-5 for the application layer security mechanism for IEC 60870-5-101/104 and IEEE 1815 (DNP3)

The requirements for the management of symmetric group keys in the context of power system communication protocols is specified in IEC 62351-6 for utilizing group security to protect GOOSE and SV communication. IEC 62351-9 utilizes GDOI as already IETF specified group-based key management protocol to manage the group security parameter and enhances this protocol to carry the security parameter for GOOSE, SV, and PTP.

This document also defines security events for specific conditions which could identify issues which might require error handling. However, the actions of the organisation in response to these error conditions are beyond the scope of this document and are expected to be defined by the organizations security policy.

In the future, as public-key cryptography becomes endangered by the evolution of quantum computers, this document will also consider post-quantum cryptography to a certain extent. Note that at this time being no specific measures are provided.

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*

IEC 62351-3:—[1], *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62351-14:—[2], *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging*

ISO/IEC 9594-8:2020, Rec. ITU-T X.509 (2019), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 9594-11:2020, Rec. ITU-T X.510 (2020), *Information technology – Open systems interconnection – The Directory: Protocol specifications for secure operations*

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*

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

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

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

IETF RFC 6407, *The Group Domain of Interpretation*

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

IETF RFC 7030, *Enrolment over Secure Transport*

IETF RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security*

_____

[1] Under preparation. Stage at the time of publication: IEC/RFDIS 62351-3:2023.

[2] Under preparation. Stage at the time of publication: IEC/ACDV 62351-14:2023.

IETF RFC 8263, *Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message*

IETF RFC 8894, *Simple Certificate Enrolment Protocol*

SOMMAIRE

AVANT-PROPOS 150
1 Domaine d'application 152
2 Références normatives 153
3 Termes, définitions et abréviations 154
3.1 Termes et définitions 154
3.2 Abréviations et acronymes 160
4 Concepts de sécurité applicables aux systèmes de puissance 161
4.1 Généralités 161
4.2 Objectifs de sécurité 161
4.2.1 Confidentialité 161
4.2.2 Intégrité des données 162
4.2.3 Authentification 162
4.2.4 Non-répudiation 162
4.3 Algorithmes cryptographiques et concepts associés 163
5 Techniques d'établissement et de gestion des clés 164
5.1 Généralités 164
5.2 Cycle de vie de la gestion de clés 164
5.2.1 Gestion de clés pendant le cycle de vie d'un dispositif 164
5.2.2 Cycle de vie d'une clé cryptographique 166
5.3 Utilisation des clés cryptographiques 168
5.4 Politique de sécurité du système de gestion de clés 168
5.5 Principes de conception de la gestion de clés pour les opérations des systèmes de puissance 168
5.6 Établissement de clés symétriques 169
5.6.1 Vue d'ensemble 169
5.6.2 Méthode d'accord de clé Diffie-Hellman 170
5.6.3 Méthode de la fonction de dérivation de la clé (KDF) 170
5.6.4 Gestion des clés de groupe 170
5.7 Confiance basée sur des infrastructures de clé publiques (PKI) et des infrastructures de gestion de privilèges (PMI) 174
5.7.1 Généralités 174
5.7.2 Autorités d'enregistrement (RA) 174
5.7.3 Autorité de certification (CA) 174
5.7.4 Certificats de clé publique 175
5.7.5 Certificats d'attribut 176
5.7.6 Extensions de certificat de clé publique et de certificat d'attribut 177
5.8 Gestion des certificats de clé publique 177
5.8.1 Processus de gestion de certificats 177
5.8.2 Création d'un certificat initial 178
5.8.3 Intégration d'une entité 178
5.8.4 Enregistrement d'une entité 179
5.8.5 Traitement d'une demande de signature de certificat (CSR) 182
5.8.6 Protocoles d'enregistrement 185
5.8.7 Protocole de gestion des ancres de confiance (TAMP) 186
5.9 Révocation de certificats de clé publique 187
5.9.1 Listes de révocation de certificats (CRL) 187
5.9.2 Protocole d'état de certificat en ligne (OCSP) 188

5.9.3 Protocole de validation de certificat fondée sur le serveur (SCVP) 190
5.9.4 Récupération de la révocation de certificat d'une entité finale 191
5.10 Confiance découlant des certificats (autosignés) délivrés hors PKI 192
5.11 Listes d'autorisation et de validation 192
5.11.1 Généralités 192
5.11.2 AVL dans les environnements non contraints 193
5.11.3 AVL dans les environnements contraints 193
6 Gestion des clés (normative) 193
6.1 Généralités 193
6.2 Traitement des événements de sécurité 193
6.3 Matériel cryptographique exigé 194
6.4 Génération de nombres aléatoires 194
6.5 Identificateurs d'objet 194
6.5.1 Concept d'identificateur d'objet 194
6.5.2 Utilisation des identificateurs d'objet par le présent document 195
7 Gestion de clés asymétriques (normative) 195
7.1 Généralités 195
7.2 Composants des certificats 195
7.2.1 Composants des certificats de clé publique 195
7.2.2 Composants des certificats d'attributs 197
7.3 Génération et installation des certificats 198
7.3.1 Génération et installation des clés privées et publiques 198
7.3.2 Protection des clés cryptographiques 198
7.3.3 Utilisation de l'infrastructure existante de gestion des clés de sécurité 199
7.3.4 Politique de certification 199
7.3.5 Enregistrement d'entité pour l'établissement d'identité 199
7.3.6 Configuration d'entité 199
7.3.7 Enregistrement d'entité 200
7.3.8 Mise à jour des informations d'ancre de confiance 202
7.4 Composants des certificats et vérification associée 203
7.4.1 Généralités 203
7.4.2 Format et codage du certificat 203
7.4.3 Vérification de la signature de certificat 203
7.4.4 Composants des certificats de clé publique 203
7.4.5 Composants des certificats d'attributs 211
7.4.6 Vérification de l'état de révocation des certificats 215
7.5 Révocation des certificats 216
7.6 Expiration et renouvellement des certificats 217
7.7 Synchronisation et exactitude des horloges 217
7.8 Listes d'autorisation et de validation 217
7.8.1 Généralités 217
7.8.2 Syntaxe des listes d'autorisation et de validation (AVL) pour les certificats de clé publique 218
7.8.3 Restriction du domaine d'application des AVL 219
7.8.4 Extension de restriction de protocole d'AVL 219
7.8.5 Marquage AVL du certificat et de l'identificateur associé 220
7.8.6 Extensions des certificats de clé publique liées à l'utilisation d'AVL 220
7.8.7 Émission d'une AVL 221
7.8.8 Traitement de bout en bout des AVL 221

8 Gestion des clés de groupe (normative) 221
8.1 Exigences relatives au GDOI 221
8.2 Protocole d'échange de clés Internet version 1 (IKEv1) 222
8.3 Échange IKEv1 de phase 1 de type 2 en mode principal 223
8.3.1 Généralités 223
8.3.2 Charge utile Certificate Request 224
8.3.3 Échange d'association de sécurité (1) 224
8.3.4 Échange de clés (2) 225
8.3.5 Échange d'authentification d'ID (3) 226
8.4 Échange informationnel ISAKMP de phase 1/2 de type 5 227
8.4.1 Généralités 227
8.4.2 Échange informationnel de phase 1 227
8.4.3 Échange informationnel de phase 2 228
8.5 Échange GROUPKEY-PULL du GDOI de phase 2 de type 32 229
8.5.1 Généralités 229
8.5.2 Calculs de hachage 230
8.5.3 Algorithme de chiffrement multi-expéditeur et de mode compteur 231
8.5.4 Prise en charge des charges utiles liées au téléchargement de clé SA KEK, SEQ, KEK/LKH 231
8.5.5 Échange de demande de SA du groupe GROUPKEY-PULL 231
8.5.6 Charge utile SA TEK 237
8.5.7 Charge utile SA TEK IEC 61850 237
8.5.8 Charge utile SA TEK pour l'IEC 61850-9-3 239
8.5.9 Présentation du SPI 241
8.5.10 Attributs de données de SA 242
8.5.11 Échange de téléchargement de clé du groupe GROUPKEY-PULL 242
8.5.12 Gestion des téléchargements de clé de TEK 245
8.6 Échange GROUPKEY-PUSH de phase 2 de type 33 245
8.6.1 Généralités 245
8.6.2 Message GROUPKEY-PUSH 246
8.6.3 Message d'acquittement GROUPKEY-PUSH 246
8.7 Aspects opérationnels 247
8.7.1 Généralités 247
8.7.2 Politique de sécurité de groupe 247
8.7.3 Dynamique de groupe 248
8.7.4 Gestion de l'assurance de livraison de clé (informative) 250
9 Déclarations de conformité d'instance de protocole (PICS) 250
9.1 Généralités 250
9.2 Notation 250
9.3 Conformité aux exigences de gestion générale des clés 251
9.4 Conformité aux exigences de gestion des clés asymétriques 251
9.5 Exigences relatives à la gestion des clés de groupe 252
9.6 OID de charge utile GDOI pris en charge 253
Annex A (informative) Relations avec les autres parties de l'IEC 62351 et autres documents de l'IEC 254
Annex B (informative) Algorithmes et mécanismes cryptographiques 256
B.1 Confiance et ancre de confiance 256
B.2 Algorithmes cryptographiques 256
B.2.1 Introduction 256

B.2.2 Force de la sécurité 258
B.3 Algorithmes de clé publique 258
B.3.1 Généralités 258
B.3.2 Algorithme de clé publique RSA 258
B.3.3 Algorithme de clé publique DSA 259
B.3.4 Algorithme de clé publique ECDSA 259
B.3.5 Algorithmes de clé publique EdDSA 261
B.3.6 Algorithmes de signature numérique 263
B.4 Algorithmes de clés symétriques 266
B.4.1 Chiffrement de flux/chiffrement de bloc 266
B.4.2 Norme de chiffrement avancé 266
B.4.3 Norme de chiffrement avancé – enchaînement de blocs de chiffrement (AES-CBC) 267
B.4.4 Norme de chiffrement avancé – mode compteur (AES-CTR) 268
B.5 Algorithmes de hachage 268
B.6 Algorithmes à valeur de contrôle d'intégrité (ICV) 269
B.6.1 Généralités 269
B.6.2 Algorithme de code d'authentification de message par hachage numérique (HMAC) 270
B.6.3 Algorithme AES-GMAC (norme de chiffrement perfectionné – code d'authentification de message avec le mode Galois) 270
B.7 Algorithmes de chiffrement authentifié avec données associées (AEAD) 271
B.7.1 Généralités 271
B.7.2 Norme de chiffrement avancé (AES) – mode Galois/compteur (GCM) 271
B.7.3 Norme de chiffrement avancé (AES) – Compteur avec CMS-MAC (CCM) 272
B.8 Accord de clé Diffie-Hellman 272
B.8.1 Généralités 272
B.8.2 Introduction aux groupes cycliques 273
B.8.3 Méthode Diffie-Hellman sur champ fini 273
B.8.4 Problème du logarithme discret 274
B.8.5 Accord de Diffie-Hellman à courbe elliptique 274
B.8.6 Algorithmes d'établissement de clé 274
B.9 Dérivation de clé 276
B.10 Migration d'algorithmes cryptographiques 276
B.11 Cryptographie de calcul post-quantique 277
B.12 Génération de nombres aléatoires (RNG) 277
B.12.1 Types de générations de nombres aléatoires 277
B.12.2 Générateurs de bits aléatoires déterministes 278
B.12.3 Génération de nombres aléatoires non déterministes 279
B.12.4 Sources d'entropie 279
Annex C (informative) Diagrammes d'enregistrement et de renouvellement de certificat 280
C.1 Enregistrement de certificat 280
C.2 Renouvellement de certificat 281
Annex D (informative) Mise en correspondance des événements de sécurité avec l'IEC 62351-14 282
D.1 Généralités 282
D.2 Enregistrements du journal des événements de sécurité pour le transport et l'enregistrement des accréditations 282

D.3 Enregistrements du journal des événements de sécurité pour la vérification du certificat de clé publique 284
D.4 Enregistrements du journal des événements de sécurité pour la vérification du certificat d'attribut 287
D.5 Enregistrements du journal des événements de sécurité pour l'état de révocation des certificats 289
D.6 Enregistrements du journal des événements de sécurité pour la gestion des clés de groupe avec le GDOI 290
Bibliographie 291

Figure 1 – Vue d'ensemble de la gestion de clés pendant le cycle de vie d'une entité 165
Figure 2 – Cycle de vie d'une clé cryptographique 166
Figure 3 – Vue d'ensemble de la gestion des clés de groupe dans l'exemple de GDOI 171
Figure 4 – Phase 1 IKE du GDOI – Authentification et sécurisation du canal de communication 172
Figure 5 – Phase 2 de la méthode PULL du GDOI 173
Figure 6 – Vue d'ensemble de l'infrastructure PKI et exemples de réalisation 174
Figure 7 – Génération centralisée de certificats 176
Figure 8 – Relation entre les certificats de clé publique et les certificats d'attribut 177
Figure 9 – Exemple d'enregistrement de l'entité SCEP et processus de demande de signature de certificat (CSR) 180
Figure 10 – Exemple d'enregistrement de l'entité EST et processus de demande de signature de certificat (CSR) 181
Figure 11 – Traitement d'une CSR 182
Figure 12 – Format d'une demande de certification 183
Figure 13 – Format de message de demande de certificat 184
Figure 14 – Liste de révocation de certificats 187
Figure 15 – Vue d'ensemble du protocole d'état de certificat en ligne (OCSP) 188
Figure 16 – Schéma utilisant une combinaison de CRL et de processus OCSP 189
Figure 17 – Flux d'appels du protocole d'état de certificat en ligne (OCSP) 190
Figure 18 – Vue d'ensemble du protocole SCVP utilisant le système principal OCSP 191
Figure 19 – Échange IKEv1 en mode principal (RFC 2409) avec des signatures numériques RSA 223
Figure 20 – Échange IKEv1 en mode principal et messages d'association de sécurité 224
Figure 21 – Échange IKEv1 en mode principal: messages d'échange de clés 225
Figure 22 – Échange IKEv1 en mode principal: messages d'authentification ID 226
Figure 23 – Calcul d'IKEv1 HASH_I 227
Figure 24 – Échange informationnel de phase 1 (voir RFC 2408, section 4.8) 228
Figure 25 – Échange informationnel de phase 2 (voir RFC 2409, section 5.7) 229
Figure 26 – Calcul d'IKEv1 HASH(1) 229
Figure 27 – Échange GROUPKEY-PULL du GDOI tel que défini dans la RFC 6407 230
Figure 28 – Calculs de hachage GROUPKEY-PULL 231
Figure 29 – Échange de demande de SA initiale du groupe GROUPKEY-PULL 232
Figure 30 – Charge utile Identification (RFC 6407) 232

Figure 31 – Données d'identification ID_OID 233
Figure 32 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF 234
Figure 33 – IPADDRESS ASN.1 BNF 234
Figure 34 – Exemple de données ASN.1 IecUdpAddrPayload avec codage DER 235
Figure 35 – Charge utile ASN.1 BNF 61850_UDP_TUNNEL 235
Figure 36 – Charge utile ASN.1 BNF 61850_ETHERNET_GOOSE/SV 235
Figure 37 – Charge utile SA TEK (RFC 6407) 237
Figure 38 – Charge utile SA TEK IEC-61850 238
Figure 39 – Corrélation de la valeur de SPI 241
Figure 40 – Échange de téléchargement de clé du groupe GROUPKEY-PULL 242
Figure 41 – Calculs de hachage de téléchargement de clé du groupe GROUPKEY-PULL 242
Figure 42 – Renouvellement de clé déclenché par les entités 244
Figure 43 – Message GROUPKEY-PUSH (RFC 6407) 245
Figure 44 – Message ACK GROUPKEY-PUSH (RFC 8263) 245
Figure 45 – Calculs de hachage ACK GROUPKEY-PUSH 246
Figure 46 – Calculs de ack_key GROUPKEY-PUSH 246
Figure A.1 – Relation entre l'IEC 62351-9 et les autres parties de l'IEC 62351 254
Figure C.1 – Enregistrement de certificat (général) 280
Figure C.2 – Diagramme d'états de renouvellement de certificat 281

Tableau 1 – Composants des certificats de clé publique 195
Tableau 2 – Composants des certificats d'attributs 197
Tableau 3 – Exigences IKEv1 du KDC 222
Tableau 4 – ID d'objet IEC 61850: obligatoire (o) et facultatif (f) 233
Tableau 5 – PICS pour la gestion générale des clés 251
Tableau 6 – PICS pour la gestion des clés asymétriques 252
Tableau 7 – PICS pour la gestion des clés de groupe (valable pour le KDC et le client) 252
Tableau 8 – PICS pour les OID pris en charge pour la charge utile Identification 253
Tableau D.1 – Journaux des événements de sécurité pour le transport des accréditations et l'enregistrement des certificats par rapport à l'IEC 62351-14 283
Tableau D.2 – Journaux des événements de sécurité définis pour la vérification du certificat de clé publique par rapport à l'IEC 62351-14 284
Tableau D.3 – Journaux des événements de sécurité définis pour la vérification du certificat d'attribut par rapport à l'IEC 62351-14 287
Tableau D.4 – Journaux des événements de sécurité définis pour l'état de révocation des certificats par rapport à l'IEC 62351-14 289
Tableau D.5 – Journaux des événements de sécurité pour le GDOI par rapport à l'IEC 62351-14 290

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 Électrotechnique 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. À 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 du présent document 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.

L'IEC 62351-9 a été établie par le WG 15, Sécurité des communications et des données, du comité d'études 57 de l'IEC, Gestion des systèmes de puissance et échanges d'informations associés. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2017. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) des composants de certificats et leur vérification ont été ajoutés;
b) le GDOI a été mis à jour pour inclure les résultats des essais d'interopérabilité;
c) des aspects liés au fonctionnement du GDOI ont été ajoutés;
d) la prise en charge du GDOI pour PTP (IEEE 1588) a été ajoutée comme spécifié par le profil de puissance de l'IEC/IEEE 61850-9-3;
e) l'enregistrement des événements de cybersécurité a été ajouté, ainsi que la mise en correspondance avec l'IEC 62351-14;
f) l'Annex B qui fournit des informations sur les algorithmes et mécanismes cryptographiques utilisés a été ajoutée.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2579/FDIS	57/2594/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

NOTE Les caractères d'imprimerie suivants sont employés:

Notation de syntaxe abstraite numéro un (ASN.1): en type `courier new` et **`bold 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 webstore.iec.ch dans les données relatives au document recherché. À 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 ce document 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 spécifie la gestion des clés cryptographiques, principalement axée sur la gestion des clés à long terme, qui sont le plus souvent des paires de clés asymétriques, telles que des certificats de clés publiques et les clés privées correspondantes. Comme les certificats constituent la base, le présent document établit une fondation pour de nombreux services de l'IEC 62351 (voir également Annex A). La gestion des clés symétriques est également prise en compte, mais uniquement en ce qui concerne les clés de session pour les communications de groupe, telles qu'elles sont appliquées dans l'IEC 62351-6. L'objectif du présent document est de définir les exigences et les technologies permettant d'assurer l'interopérabilité de la gestion des clés en spécifiant ou en limitant les options de gestion de clés à utiliser.

Le présent document présume qu'une organisation (ou un groupe d'organisations) a défini une politique de sécurité pour sélectionner le type de clés et d'algorithmes cryptographiques qui seront utilisés, qui peuvent être à aligner sur d'autres normes ou exigences réglementaires. Le présent document spécifie donc uniquement les techniques de gestion de ces infrastructures de clé et de cryptographie sélectionnées. Le présent document présume que le lecteur a des notions de base en cryptographie et sur les principes de gestion des clés.

Les exigences relatives à la gestion des paires de clés (de session) symétriques dans le contexte des protocoles de communication sont spécifiées dans les parties de l'IEC 62351 qui utilisent ou spécifient une communication par paire, telles que:

- l'IEC 62351-3 pour TLS en profilant les options TLS;
- l'IEC 62351-4 pour la sécurité de bout en bout de la couche application;
- l'IEC 62351-5 pour le mécanisme de sécurité de la couche application pour l'IEC 60870-5-101/104 et l'IEEE 1815 (DNP3).

Les exigences relatives à la gestion des clés de groupe symétriques dans le contexte des protocoles de communication des systèmes de puissance sont spécifiées dans l'IEC 62351-6 pour l'utilisation de sécurité de groupe pour protéger les communications GOOSE et SV. L'IEC 62351-9 utilise GDOI comme protocole de gestion de clés par groupe déjà spécifié par l'IETF (Internet Engineering Task Force) pour gérer le paramètre de sécurité de groupe et améliore ce protocole pour transporter le paramètre de sécurité pour les communications GOOSE, SV et PTP.

Le présent document définit également les événements de sécurité pour des conditions spécifiques susceptibles d'identifier des problèmes pouvant exiger un traitement des erreurs. Cependant, les actions de l'organisation en réponse à ces conditions d'erreur ne relèvent pas du domaine d'application du présent document et sont censées être définies par la politique de sécurité des organisations.

À l'avenir, lorsque la cryptographie à clé publique sera mise en danger par l'évolution des ordinateurs quantiques, le présent document examinera également la cryptographie post-quantique dans une certaine mesure. Il est à noter qu'à l'heure actuelle, aucune mesure spécifique n'est prévue.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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)

IEC 62351-3:— [1], *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP*

IEC 62351-4, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 4: Profils comprenant le MMS et ses dérivés*

IEC 62351-5, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 5: Aspects de sécurité pour l'IEC 60870- 5 et ses dérivés*

IEC 62351-6, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850*

IEC 62351-14:— [2], *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging* (disponible en anglais seulement)

ISO/IEC 9594-8:2020, Rec. UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Partie 8: Cadre général des certificats de clé publique et d'attribut*

ISO/IEC 9594-11:2020, Rec. UIT-T X.510 (2020), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire – Partie 11: Spécifications de protocole pour un fonctionnement sécurisé*

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 – Partie 1: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationale*

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

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization* (disponible en anglais seulement)

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

IETF RFC 6407, *The Group Domain of Interpretation* (disponible en anglais seulement)

_____

[1] En cours d'élaboration. Stade au moment de la publication: IEC/RFDIS 62351-3:2023.

[2] En cours d'élaboration. Stade au moment de la publication: IEC/ACDV 62351-14:2023.

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

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

IETF RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security* (disponible en anglais seulement)

IETF RFC 8263, *Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message* (disponible en anglais seulement)

IETF RFC 8894, *Simple Certificate Enrolment Protocol* (disponible en anglais seulement)