

# 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**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2023 IEC, Geneva, Switzerland

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

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

#### IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

If you wish to give us your feedback on this publication or request further assistance, please contact the Customer Service Centre: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC Products & Services Portal - [products.iec.ch](http://products.iec.ch)

Discover our powerful search engine and read freely all the publications preview. With a subscription you will always have access to up-to-date content tailored to your needs.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

### A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

#### Recherche de publications IEC -

[webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

#### IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [sales@iec.ch](mailto:sales@iec.ch).

#### IEC Products & Services Portal - [products.iec.ch](http://products.iec.ch)

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

# 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 978-2-8322-6950-3

**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.**

## 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 algorithm.....	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 – IP\_ADDRESS 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 .....	63
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. For 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 Publications"). 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 far 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 TC77: 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](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/publications](http://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](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 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.