BS EN IEC 62351-9:2023

BSI Standards Publication

# Power systems management and associated information exchange — Data and communications security

Part 9: Cyber security key management for power system equipment

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

# National foreword

This British Standard is the UK implementation of EN IEC 62351-9:2023. It is identical to IEC 62351-9:2023. It supersedes BS EN 62351-9:2017, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its committee manager.

**Contractual and legal considerations**

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 13656 2

ICS 33.200

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2023.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN IEC 62351-9

July 2023

ICS 33.200

Supersedes EN 62351-9:2017

English Version

# Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment (IEC 62351-9:2023)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance (IEC 62351-9:2023)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 9: Cyber security Schlüssel-Management für Stromversorgungsanlagen (IEC 62351-9:2023)

This European Standard was approved by CENELEC on 2023-07-11. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

© 2023 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62351-9:2023 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

# European foreword

The text of document 57/2579/FDIS, future edition 2 of IEC 62351-9, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62351-9:2023.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2024-04-11
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2026-07-11

This document supersedes EN 62351-9:2017 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

## Endorsement notice

The text of the International Standard IEC 62351-9:2023 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

| | | |
|---|---|---|
| ISO/IEC 19790:2012 | NOTE | Approved as EN ISO/IEC 19790:2020 (not modified) |
| IEC 62351-8 | NOTE | Approved as EN IEC 62351-8 |
| ISO/IEC 19790 | NOTE | Approved as EN ISO/IEC 19790 |
| IEC 62443-3-3 | NOTE | Approved as EN IEC 62443-3-3 |
| IEC 62443-4-2 | NOTE | Approved as EN IEC 62443-4-2 |



Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

# Annex ZA
(normative)

## Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cencenelec.eu.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC/TS 62351-2 | - | Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms | - | - |
| IEC 62351-3 | 2023 | 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 | EN IEC 62351-4 | - |
| IEC 62351-5 | - | Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives | EN IEC 62351-5 | - |
| IEC 62351-6 | - | Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850 | EN IEC 62351-6 | - |
| IEC 62351-14 | —[1] | Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging | - | - |
| ISO/IEC 9594-8 | 2020 | Information technology - Open systems interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks | - | - |
| ISO/IEC 9594-11 | 2020 | Information technology - Open systems interconnection directory - Part 11: Protocol specifications for secure operations | - | - |

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



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| ISO/IEC 9834-1 | 2012 | 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 | - | - |
| IETF RFC 8263 | - | Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message | - | - |
| IETF RFC 8894 | - | Simple Certificate Enrolment Protocol | - | - |



Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

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

AVA Documents
Document Sharing Hub

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) ....

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

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;

Documents
Document Sharing Hub

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.**

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

# 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.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

## 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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

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

IETF RFC 8894, *Simple Certificate Enrolment Protocol*

# 3 Terms, definitions, and abbreviations

## 3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

**3.1.1**
**asymmetric keys**
two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification

**3.1.2**
**authorization and validation list**
AVL
signed list containing information to an AVL entity about potential communications entities and possible restrictions on the communications with such entities

[SOURCE: ISO/IEC 9594-8:2020, 3.5.9]

**3.1.3**
**authorization and validation list entity**
AVL entity
entity, when acting as a relying party, which is dependent on an AVL issued by a designated authorizer

[SOURCE: ISO/IEC 9594-8:2020, 3.5.10]

**3.1.4**
**authorizer**
entity trusted by one or more entities operating as AVL entities to create, maintain and sign authorization and validation lists

[SOURCE: ISO/IEC 9594-8:2020, 3.5.11]

**3.1.5**
**certification path**
ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the end-entity public-key certificate to be validated

Note 1 to entry: All intermediate public-key certificates, if any, are CA certificates in which the subject of the preceding public-key certificate is the issuer of the following public-key certificate.

[SOURCE: ISO/IEC 9594-8:2020, 3.5.21]

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

**3.1.6**
**certification request**
request issued when a new public-key certificate or renewal of a public-key certificate is required

[SOURCE: IETF RFC 2986]

**3.1.7**
**controllership**
intersection of legal ownership, physical control, and logical control over a device or system, in which the nature of any contractual agreements between ownership and control of the device or system is not important in the context

**3.1.8**
**cryptographic binding**
use of one or more cryptographic techniques by a CKMS to establish a trusted association between a key and selected metadata elements

[SOURCE: NIST SP 800-130]

**3.1.9**
**dataset**
collection of data

**3.1.10**
**device**
component implementing specific functionalities, which may act as a client (e.g., TLS client) or a server (e.g., key distribution centre for GDOI)

**3.1.11**
**digital signature**
result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation

[SOURCE: FIPS 186]

**3.1.12**
**end entity (PKI)**
entity that has been assigned an end-entity public-key certificate, where the private key cannot be used to sign other public-key certificates, but may be used for signing for other purposes

**3.1.13**
**entity**
generic term that covers human users, automation systems, software applications, communication nodes, field devices, and other types of assets

**3.1.14**
**fingerprint**
hash result ("key fingerprint") used to authenticate a public key or other data

[SOURCE: IETF RFC 4949]

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

**3.1.15**
**group controller/key server**
GCKS
device that defines group policy and distributes keys for that policy

[SOURCE: IETF RFC 3740]

**3.1.16**
**group domain of interpretation**
GDOI
domain that manages group security associations, which are used by IPsec and potentially other data security protocols

Note 1 to entry: These security associations protect one or more key-encrypting keys (KEK), traffic-encrypting keys (TEK), or data shared by group members. GDOI uses the notion of a group controller, which is used to support the establishment of security associations between members of a group.

[SOURCE: IETF RFC 6407]

**3.1.17**
**group member**
GM
authorized member of a secure group, sending and/or receiving IP packets related to the group

**3.1.18**
**hash function**
(mathematical) function which maps data of arbitrary size into data of a fixed size called a digest

**3.1.19**
**hash message authentication code**
HMAC
cryptographic code used for authentication with symmetric keys and for data integrity

[SOURCE: IETF RFC 2104]

**3.1.20**
**key distribution centre**
KDC
centre which, in an IEC 62351-9 context, provides a network service that supplies temporary (symmetrical) session keys to predefined set of peers after successful authentication

Note 1 to entry: This is also known as Group Controller/Key Server (GCKS) (See GDOI).

**3.1.21**
**key management system**
system for the management (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction) of cryptographic keys and their metadata

**3.1.22**
**message authentication code**
MAC
cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modification of the data

[SOURCE: SP 800-63; FIPS 201]

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

**3.1.23**
**object identifier**
ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node

[SOURCE: ISO/IEC 9834-1:2012, 3.5.11]

**3.1.24**
**online certificate status protocol**
OCSP
protocol that enables applications to determine the (revocation) state of an identified certificate

Note 1 to entry: OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.

[SOURCE: IETF RFC 6960]

**3.1.25**
**operator**
particular type of user that is usually responsible for the correct operation of the equipment under control

**3.1.26**
**pre-shared key**
PSK
secret which is shared in advanced between the two entities, such as software applications or devices, to be able to authenticate themselves or to establish a secure connection

**3.1.27**
**private key**
(in a public-key cryptosystem) that key of an entity's key pair which is known only by that entity

[SOURCE: ISO/IEC 9594-8:2020, 3.5.50]

**3.1.28**
**public-key certificate**
public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it

Note 1 to entry: A public-key certificate is often called an X.509 certificate or a digital certificate. However, such terms are ambiguous, as they could also mean attribute certificates, which are also defined by ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019).

[SOURCE: ISO/IEC 9594-8:2020, 3.5.58, modified – Note 1 to entry added]

**3.1.29**
**public-key cryptography standards**
PKCS
specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography

[SOURCE: www.rsa.com]

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

**3.1.30**
**random number generation**
RNG
process used to generate an unpredictable series of numbers

Note 1 to entry: Each individual value is called random if each of the values in the total population of values has an equal probability of being selected.

[SOURCE: NIST SP 800-57]

**3.1.31**
**registration authority**
RA
those aspects of the responsibilities of a certification authority that are related to identification and authentication of the subject of a public-key certificate to be issued by that certification authority

Note 1 to entry: An RA may either be a separate entity or be an integrated part of the certification authority.

Note 2 to entry: This definition is different in scope from the one defined in Rec. ITU-T X.660 | ISO/IEC 9834-1.

[SOURCE: ISO/IEC 9594-8:2020, 3.5.61]

**3.1.32**
**relying party**
entity that relies on the data in a public-key certificate in making decisions

[SOURCE: ISO/IEC 9594-8:2020, 3.5.62]

**3.1.33**
**security association**
SA
relationship established between two or more entities to enable them to protect data they exchange

[SOURCE: NIST IR 7298 Rev.1]

**3.1.34**
**security strength**
ability of the security technologies to make it infeasible for a would-be attacker to bypass or subvert

Note 1 to entry: This is often measured in bits of security.

[SOURCE: NIST SP 800-130]

**3.1.35**
**session key**
in the context of symmetric encryption, key that is temporary or is used for a relatively short period of time

[SOURCE: IETF RFC 2828]

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

**3.1.36**
**symmetric key**
cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or to create a message authentication code and to verify the code

[SOURCE: NIST SP 800-63]

**3.1.37**
**trust**
firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context

**3.1.38**
**trust anchor**
entity that is trusted by a relying party and used for validating public-key certificates in certification paths

[SOURCE: ISO/IEC 9594-8:2020, 3.5.72]

**3.1.39**
**trust anchor information**
at least the: distinguished name of the trust anchor, associated public key, algorithm identifier, public key parameters (if applicable), and any constraints on its use including a validity period

Note 1 to entry: The trust anchor information may be provided as a self-signed CA-certificate or as a normal CA-certificate (i.e., cross-certificate).

[SOURCE: ISO/IEC 9594-8:2020, 3.5.73]

**3.1.40**
**trust anchor store**
trust anchor information collection at a relying party for one or more trust anchors

[SOURCE: ISO/IEC 9594-8:2020, 3.5.74]

## 3.2 Abbreviations and acronyms

Additional abbreviations and acronyms are given in IEC TS 62351-2.

| | |
|---|---|
| AA | Attribute Authority |
| AEAD | Authenticated Encryption with Associated Data |
| ASN.1 | Abstract Syntax Notation One |
| AVL | Authorization and Validation List |
| AVMP | Authorization and Validation Management Protocol |
| BRSKI | Bootstrapping of Remote Secure Key Infrastructures |
| CA | Certification Authority |
| CASP | Certification Authority Subscription Protocol |
| CIA | Confidentiality, Integrity, and Availability |
| CMC | Certificate Management over CMS |
| CMS | Cryptographic Message Syntax |
| CPS | Certificate Practice Statement |
| CSR | Certificate Signing Request (also referred in the context of a certification request) |
| DER | Distinguished Encoding Rules |

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

| | |
|---|---|
| DOI | Domain of Interest |
| DSA | Digital Signature Algorithm |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EdDSA | Edwards-curve Digital Signature Algorithm |
| EST | Enrolment over Secure Transport |
| FQDN | Fully Qualified Domain Name |
| GCKS | Group Controller/Key Server |
| GAP | Group Associated Policy |
| GCM | Galois Counter Mode |
| GDOI | Group Domain of Interpretation |
| GKDC | Group KDC |
| GM | Group Member |
| GMAC | Galois Message Authentication Code |
| GOOSE | Generic Object-Oriented Substation Event |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| ICV | Integrity Check Value |
| IDevID | Initial Device Identifier (IEEE 802.1AR) |
| IED | Intelligent Electronic Device |
| ID | Identity |
| IKE | Internet Key Exchange |
| ISAKMP | Internet Security Association and Key Management Protocol |
| KD | Key Download |
| KDC | Key Distribution Centre, aka GKDC |
| KDF | Key Derivation Function |
| KEK | Key Encryption Key |
| LDevID | Locally significant Device Identifier (IEEE 802.1AR) |
| MUD | Manufacturer Usage Description (RFC 8520) |
| OCSP | Online Certificate Status Protocol |
| OTP | One Time Password |
| PDU | Protocol Data Unit |
| PEM | Privacy-enhanced Electronic Mail |
| PKCS | Public-Key Cryptography Standard |
| PKI | Public-Key Infrastructure |
| RA | Registration Authority |
| RNG | Random Number Generation |
| RSA | Rivest Shamir Adleman, public-key crypto system |
| SA | Security Association |
| SCEP | Simple Certificate Enrolment Protocol |
| SPI | Security Parameter Index |
| SV | Sampled Values |
| TAMP | Trust Anchor Management Protocol |
| TEK | Traffic Encryption Key |

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

# 4 Security concepts applicable to power systems

## 4.1 General

This clause is intended as an introduction to cryptographic concepts, which are applicable in power systems. It provides an overview about security objectives in power systems, which cryptographic algorithms may be utilized to meet these security objectives, and how they may be applied in different deployment environments. Moreover, this clause together with Annex B provides some background information on utilized cryptographic algorithms as well as potential boundary conditions in different environments. The normative part of this document will specify their application. Also addressed is the general handling of security events.

## 4.2 Security objectives

### 4.2.1 Confidentiality

Confidentiality is needed to prevent the access to sensitive data, particularly when it is in transit.

The cryptographic goal of data confidentiality in power system implementations is typically accomplished by encrypting the message using symmetric key cryptography. The message may be encrypted individually at the application level, at the underlying communications channel, or possibly both. As stated previously, the confidentiality of this message is dependent upon the sender and receiver maintaining the secrecy of the symmetric key. Additionally, asymmetric cryptography is often used to exchange or negotiate symmetric session keys that are valid for a specified length of time, thus reducing the risk associated with keeping a specific session key secret.

To limit the damage if a symmetric key is compromised, the symmetric key used on a connection or association is recommended to be unique. This can be achieved by using an ephemeral key negotiation as described in B.8. For TLS this can be done by the selection of appropriate cipher suites (as outlined in IEC 62351-3).

### 4.2.2 Data integrity

Data integrity concerns the detection of unauthorized changes of data during transit or at rest. It enables the verifier of the integrity check value to detect any integrity violations to the related data.

Two methods are used for detecting data integrity violation. Both methods make use of cryptographic hash functions to detect any changes in received data. As discussed in Clause B.5, a hash function results in the production of a fixed length digest over some input data. This digest changes unpredictably even for a small change in the data to be hashed. The two methods used for detecting integrity violation are:

a) Use of digital signatures as discussed in B.3.6.

b) Use of integrity check values (ICVs) as discussed in Clause B.6.

Authenticated encryption is a further variant, which provides data confidentiality and data integrity in a single operation. It is described in Clause B.7.

### 4.2.3 Authentication

When an entity receives data from some other entity, it is critical that the sender of that data is securely authenticated. This document identifies the same two methods for authentication as mentioned for data integrity in 4.2.2:

a) Use of digital signature, where a verified digital signature proves with some certainty that the sender is in the possession of the private key corresponding to the public key used for verifying the digital signature. This is further discussed in B.3.6.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

b) Use of integrity check value (ICV), where a verified ICV proves with some certainty that the sender is in possession of the same symmetric key as the recipient. The symmetric key used for generation of a ICV is established as part of the authentication process and thereby bound to that authentication. ICV is further discussed in Clause B.6.

#### 4.2.4 Non-repudiation

Non-repudiation refers to the ability to bind an action (e.g., a command or a message) irrefutably to an issuing entity. It may bind a sender to the action of sending a specific message or a receiver to the action of receiving a specific message.

The ISO/IEC 13888 series specifies different levels of non-repudiation and it specifies two distinct ways of how to establish non-repudiation:

a) ISO/IEC 13888-2 specifies procedures using symmetric-key cryptography. These techniques require the involvement of a trusted third party.

b) ISO/IEC 13888-3 specifies procedures for using asymmetric-key cryptography.

### 4.3 Cryptographic algorithms and concepts

The scope of this document is the key management for power system application comprising PKI based management of asymmetric key material as well as group based key management for symmetric keys. Key management is applicable to all parts of the IEC 62351 series which utilize cryptographic key material to protect information exchanged in power system automation protocols.

Annex B provides detailed explanations of different types of cryptographic algorithms and related concepts, such as trust, trust anchor, security level, random number generation, and migration from one cryptographic algorithm to a different (typically stronger) one. The latter becomes more important to address advances in quantum computing, which specifically endangers asymmetric cryptographic algorithms.

In addition to a general introduction to cryptographic algorithms, the following types of algorithms are considered to a certain extend:

- Asymmetric algorithms comprising RSA, ECDSA, and EdDSA algorithms, including general description, key generation, and security considerations for the different types of asymmetric algorithms.
- Symmetric key algorithms in different operational modes. Only algorithms based on advance encryption standard (AES) are considered. The operational modes considered are cipher block chaining (AES-CBC) and a mode based on a counter mechanism (AES-CTR). They are both defined for key sizes of 128 and 256 bits.
- Hash algorithms. The algorithms considered are so-called secure hash algorithms (SHAs) and only SHA-256 and SHA-512 are considered. The description includes a list of areas where hash algorithms are used.
- Algorithms to create Integrity Check Values (ICVs). Two types of ICV algorithms are relevant for this document. The first type is keyed-hash message authentication code (HMAC) algorithms which specify the use of a symmetric key and a hash algorithm. Two HMAC algorithms are included, one based on SHA-256 and one on SHA-512. The other type of ICV algorithm is the advance encryption standard – Galois message authentication code (AES-GMAC).
- Authenticated encryption with associated data (AEAD) algorithms such as AES-GCM or AES-CCM, are cryptographic algorithms that in addition to specifying encryption/decryption also provide integrity capabilities for encrypted data and also for some associated data. Two types of AEAD algorithms are included. They are both based on AES for encryption but use different techniques for generating the ICV part. They are both provided for AES key sizes of 128 and 256 bits.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

- Key agreement using Diffie Hellman to compute a shared key based on unshared private keys. Generating symmetric keys in flight is essential for key management and the Diffie-Hellman method is a much-used technique for that purpose. Two types of Diffie-Hellman schemes are provided using two different types of mathematics (prime fields and elliptic curves). They are both defined in such a way to support migrations to more secure ones.

As these algorithms and concepts are being applied in power systems, Annex B provides an overview and also background information as well as references to further information. This annex is intended as introduction material to gain a better understanding regarding the application of these algorithms in later normative clauses of this document.

# 5 Key establishment and management techniques

## 5.1 General

This clause provides an overview about techniques for the management of symmetric and asymmetric key material, connected concepts, and necessary infrastructures. For the symmetric key material, the focus is placed on the management of group-based keys. This clause builds the background for the normative description in the following clauses.

## 5.2 Key management lifecycle

### 5.2.1 Key management in the life cycle of a device

Key management is part of the life cycle of devices, typically following the flow shown in Figure 1.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

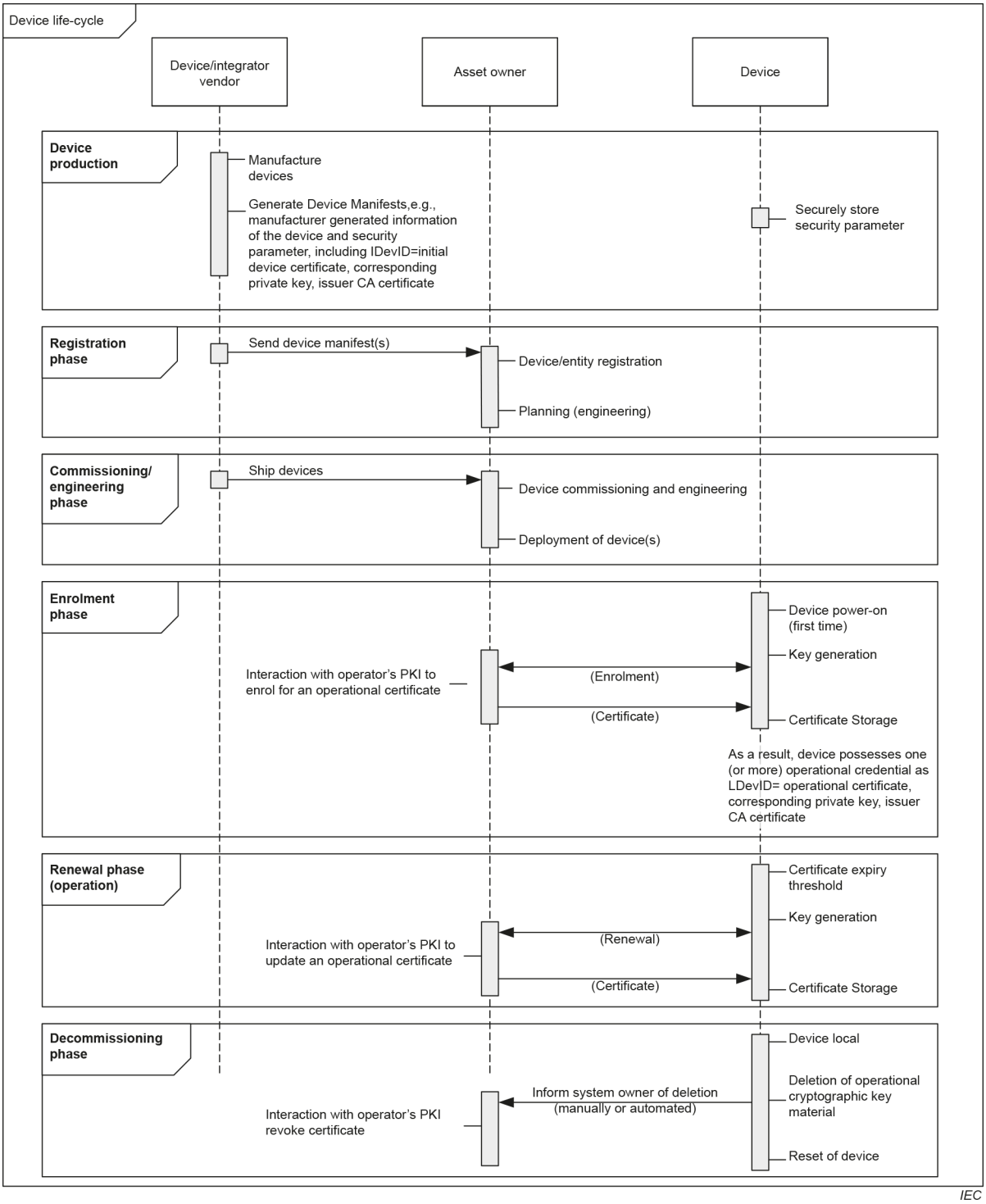


**Figure 1 – Overview key management in the life cycle of an entity**

Manufacturers can support the key management life cycle for an entity by providing a security manifest of identity information, such as a manufacturer unique identifier, or one-time-password, or certificate from a manufacturer CA, or manufacturer's entity certificate for each of their devices and systems. IEEE 802.1AR defines these initial set of credentials as IDevID (Initial Device Identifier), consisting of the initial certificate, the corresponding private key, as well as certificate chain up to the trust anchor. At each change in ownership or even status (e.g., warehoused vs. deployed), new certificates should be enrolled, providing a trusted chain of the product identity in use. When these entities are eventually engineered and deployed, their manufacturer certificates (if available) may be used to enrol the entity in operations, leading to one or more operational certificate(s) (LDevID, Local Device Identifier), which

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

enables them to authenticate and commence their information exchanges. Shortly before these operational certificates are due to expire, they should be renewed to avoid certificate verification errors.

Also, to be considered is the decommissioning of devices, which should go along with the deletion of any operational cryptographic credentials to ensure that this information cannot be misused once the device it taken out of operation. Note that the IDevID (if available), is typically not deleted.

Manufacturers are encouraged to make the process for securely wiping a device of any operational credentials (certificates, trust anchor database, etc.) and restoring the default initial set of credentials a simple process; or if necessarily complex, at least clearly documented. This would assist both with good end-of-service hygiene and where appropriate, confidence that any workshop/workbench testing credentials have been removed prior to deployment. System owners are involved in the decommission process as part of the lifecycle (see clause 5.2.2).

### 5.2.2 Lifecycle of a cryptographic key

Cryptographic keys in general and certificates specifically follow a life cycle. They are created, distributed, installed, applied, updated, and destroyed to meet the key management security policy requirements. As an example, the typical life cycle of keys found in PKI based systems is depicted in Figure 2. The general key life cycle management is discussed in more detail in ISO/IEC 11770 (cf. [6][3]) and NIST SP 800-130 [11]. The life cycle of a certificate that is typically managed, is depicted here on an abstract level. More details about certificate management can be found in 5.8.

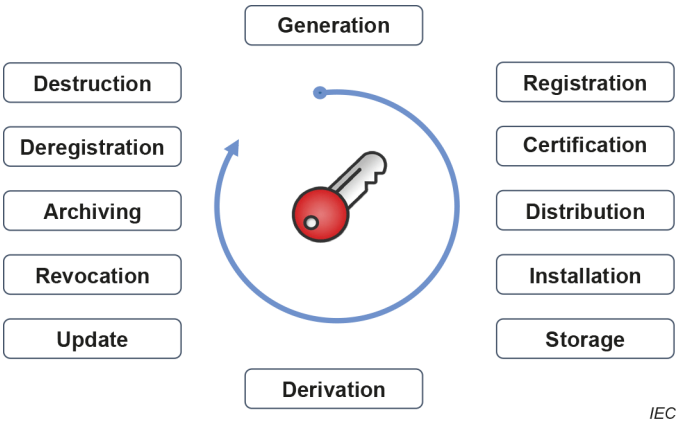


**Figure 2 – Cryptographic key life cycle**

The following list briefly describes each of the possible stages in the life cycle of a cryptographic key. All stages are required for asymmetric keys, while registration, certification, deregistration, and revocation are not required for symmetric keys:

- Generation: Cryptographic keys can be created by the entity itself if it has the appropriate capabilities. Alternatively, keys may be created externally and installed on the target entity. Often this latter approach is used if the entity cannot support one of the critical components in generating keys, namely the random number generator (RNG) which must ensure randomness to a high degree (see B.12). Keys might also need to be created externally if they must be archived (e.g., for encryption keys used for stored data). When certificates are about to expire, entities need to apply for certificate renewal.
- Registration: If certificates and the PKI process are used, registration through a Registration Authority (RA) establishes the "identity" of an entity. This is done by generating the key pair

[3] Numbers in square brackets refer to the bibliography.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

either entity local or centrally. The entity provides a certification request to the RA, which is then further processed in conjunction with the Certification Authority (CA).

- Certification: After registration of an entity by an RA, the CA provides a digitally signed certificate to the entity that thus connects its public key with the private key held by the entity. Depending on the key generation, this can be part of the key generation in a trust centre or may be done using information sent in a certification request.
- Distribution: Key distribution comprises the process to transport keys as well as key management information to authorized entities in a secure manner. Private (secret) keys, although ideally generated in end devices and thus not requiring distribution, must be distributed using secure means if externally generated. Public keys, within public-key certificates, can be distributed using non-secure means since end devices can verify their authenticity directly by verifying the certificate signature.
- Installation: A key may be installed in an entity during the manufacturing and/or engineering processes (pre-shared key) or may be installed later via on-line procedures. The latter process may require communication with a security server, out-of-band using a separate communication channel, or in-band as part of a service communication.
- Storage: The private/symmetric keys are recommended to be securely stored in the entity. Secured key storage should be compliant with FIPS 140-3 [70] or ISO/IEC 19790 [71].
- Derivation: Cryptographic keys used as session keys or other short-term keys can be derived from the private or symmetric keys that are stored in the entity.
- Update: Cryptographic keys need to be regularly updated. Cryptographic keys have a dedicated lifetime, e.g., public-key certificates issued to users may have a lifetime of 2 years, while public-key certificates issued to server may be limited to 1 year or shorter, pre-shared keys to a few weeks or months, and session keys to a few hours and/or a few thousand packets. Lifetime recommendations of cryptographic keys can be found in NIST SP 800 -57 Part 1 [73] and German BSI TR 02102-1 [58].
- Revocation: Certificate revocation may occur when a certificate is no longer authorized to be used. This may be the case if a device is removed from service or changes its role, or if a private key is compromised or suspected of being compromised.
- Archiving: Symmetric keys needed to decrypt long-term stored data should be archived in secure confidential storage to enable data recovery (to allow access to store encrypted data later). In addition, to support future signature verification, public-key certificates should also be archived, although secure confidential storage is not needed.
- De-Registration: This procedure is typically provided by the registration authority to remove the association of an entity with a dedicated key. It is typically used in the key destruction phase.
- Destruction: When a cryptographic key is destroyed, it must not be able to be recovered or used. This occurs at the end of the cryptographic key life cycle.

### 5.3 Cryptographic key usages

Cryptographic keys are used for different purposes and in different phases of the product lifecycle and are applied as:

- Public-key certificates and corresponding private keys: Used to identify, authenticate, and authorize entities. Moreover, they are often employed in the negotiation or establishment of session keys.
- Pre-shared keys (e.g., for real-time communication): Used as a shared secret between entities to secure the data exchange (integrity, confidentiality) between them. This may be useful in environments not supporting a PKI. Additionally, this scheme may be used during PKI enrolment, allowing an entity to authenticate itself against the certification authority (CA), for example when processing a certification request. *Note that the security of pre-shared key relates to their complexity.* Password complexity rules are typically given by the organization security policies.
- Session keys (pair wise or group-based): Used for efficient encryption or integrity checks on communication messages.

AVA Documents
Document Sharing Hub

- Session parameters (dedicated cryptographic algorithms): Used to support sessions (keys, lifetime, etc.).
- Cryptographic access tokens: Mostly used to transfer/provide authorization/access of resources to entities.
- Other relevant entities or organizational credentials.

### 5.4 Key management system security policy

Cryptographic keys need to be protected. Therefore, every organization (or group of organizations that expect to exchange data) should develop a security policy for its key management system that establishes and specifies all of the requirements for protecting the confidentiality, integrity, availability, and source authentication of all cryptographic keys and their associated metadata used by the organization. These protection requirements should cover the entire key life cycle, including when they are initially provided, operational, stored, and transported. A key management security policy should also include the selection of all cryptographic mechanisms and protocols to be used throughout the organization's systems.

Key management systems also need security administrative support to ensure the security policies are followed and the procedures are maintained. The specification of this support is out-of-scope for this document, but can be found in other documents such as ISO/IEC 11770 ([6]) or in NIST SP 800-130 ([11]) or in IEC 62443-4-2 [74].

### 5.5 Key management design principles for power system operations

Cryptographic keys are used to secure the communication between different system entities, such as users, systems, software applications, communication nodes, and the potentially large numbers of equipment and devices that are often located at remote, often untrusted sites, and increasingly owned/operated by different organizations

These cryptographic keys should be managed so that they can effectively and securely be provided to the entities that require secure exchanges of data. This key management needs to consider many issues, ranging from the capabilities of entities to the varied types of locations of these entities, to the timing for providing and revoking keys, to the varied ownership of the entities, to possible different regulatory jurisdictions, and to protecting the key management processes themselves from attacks.

For instance, many smaller devices are limited in computational power and memory capacity, while the communication networks may also be limited in available bandwidth. Therefore, some of the key management techniques used in traditional enterprise information technology system environments with powerful systems and high bandwidth communications are not well suited to power system automation and communication environments.

As another example, in groups of organizations that expect to exchange operational data, some of the organizations may not have the expertise or personnel to manage cryptographic keys without third party support. These realities should therefore be included in the design of key management processes.

To address these constraints, this document specifies different key management techniques that could be used for different requirements and constraints. Specifically, it specifies how to manage keys for each of the cryptographic functions specified in the other IEC 62351 parts. Sources of guidance on key management design principles include:

- Reference [6] ISO/IEC 11770-1:2010 Information technology – Security techniques – Key management – Part 1: Framework
- Reference [8] ISO/IEC 11770-3:2008 Information technology – Security techniques – Key management – Part 3: Mechanisms Using Asymmetric Techniques
- Reference [13] NIST 800-57, Part 1

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

## 5.6 Establishment of symmetric keys

### 5.6.1 Overview

Symmetric cryptographic keys are required for two reasons:

a) they are used for encryption and decryption of data during transfer; and

b) they are used for generation and verification of ICVs.

For security reasons, the keys for pair wise communication are expected to be different between any two pairs of communicating entities.. Symmetric keys between two entities may be established in different ways:

a) by means defined in other parts of IEC 62351, specifically in:
   - IEC 62351-3 for TLS, by profiling the TLS options. Here, during the TLS handshake between two entities, techniques based on public-key algorithms are used to establish a pairwise key.
   - IEC 62351-4 for the application layer end-to-end security profile. As for TLS, a pairwise key is established between two communicating entities based on public-key algorithms.
   - IEC 62351-5 for the application layer security mechanism for IEC 60870-5-101/104 and IEEE 1815 (DNP3) relying also on the application of public-key algorithms.

b) by use of key agreement for pairwise key establishment, as described in the Diffie-Hellman key agreement method (5.6.2).

c) by use of key derivation function (KDF) method (5.6.3), e.g., based on an already existing symmetric key.

d) by use of key distribution, e.g., using public key encryption as used in certain TLS cipher suites.

Symmetric keys established between two entities following a) to d) are often not directly applied to protect the communication but rather used to derive security service specific keys. In the example of IEC 62351-4 there are distinct symmetric keys available for integrity protection and also for confidentiality protection. Moreover, these keys are direction dependent resulting in multiple keys between two communicating entities. These keys also have a lifecycle requiring that the initial symmetric key is established in a secure way and also that it is managed through the lifetime of the communication connection. As outlined in the bullet list above, the establishment of symmetric keys typically supported by other methods to limit the overhead for managing pure symmetric keys between the communicating entities.

One method that can be considered for accommodating networked entities, which rely on multicast communication is group-based key management. In particular, group-based keys can be utilized in power automation systems. For this, group-based key management protocols are employed which include a key management component for managing keys and associated policies to authenticated members of a group. Group key management is described in 5.6.4.

### 5.6.2 The Diffie-Hellman key agreement method

The Diffie-Hellman key agreement method allows two parties that have to exchange so-called Diffie-Hellman public keys to jointly arrive at a shared secret in a way that does not allow an eavesdropper to learn about this shared secret.

Details on the Diffie Hellman key agreement is provided in Clause B.8 for the classical and the elliptic curve Diffie Hellman.

### 5.6.3 Key derivation function (KDF) method

A key derivation function (KDF) is a cryptographic algorithm that derives one or more symmetric keys from a secret value such as another symmetric key, a password, or a passphrase using a pseudorandom function.

AVA Documents
Document Sharing Hub

Details on KDF are provided in B.9.

### 5.6.4 Group key management

#### 5.6.4.1 Purpose of group keys

For multicast interactions between entities forming a group that have stringent performance requirements, the application of a group key is more efficient than having separate peer-to-peer relationships in that group. Also, under such circumstances, the key management is likely to be performed outside the context of the actual protocol applying the keys. Group key management typically uses a combination of asymmetric and symmetric cryptography. The asymmetric part is used to identify and authenticate the entities, while the symmetric part protects the actual key and policy transport.

To realize the setup of a group-based key, one system or device typically is designated as the group controller, which in turn authenticates other entities via their certificates or pre-shared keys. After successful authentication of the entities, the group controller distributes the actual group key to them. Hence, the group controller resembles the functionality of a Key Distribution Centre (KDC) (see Figure 3).

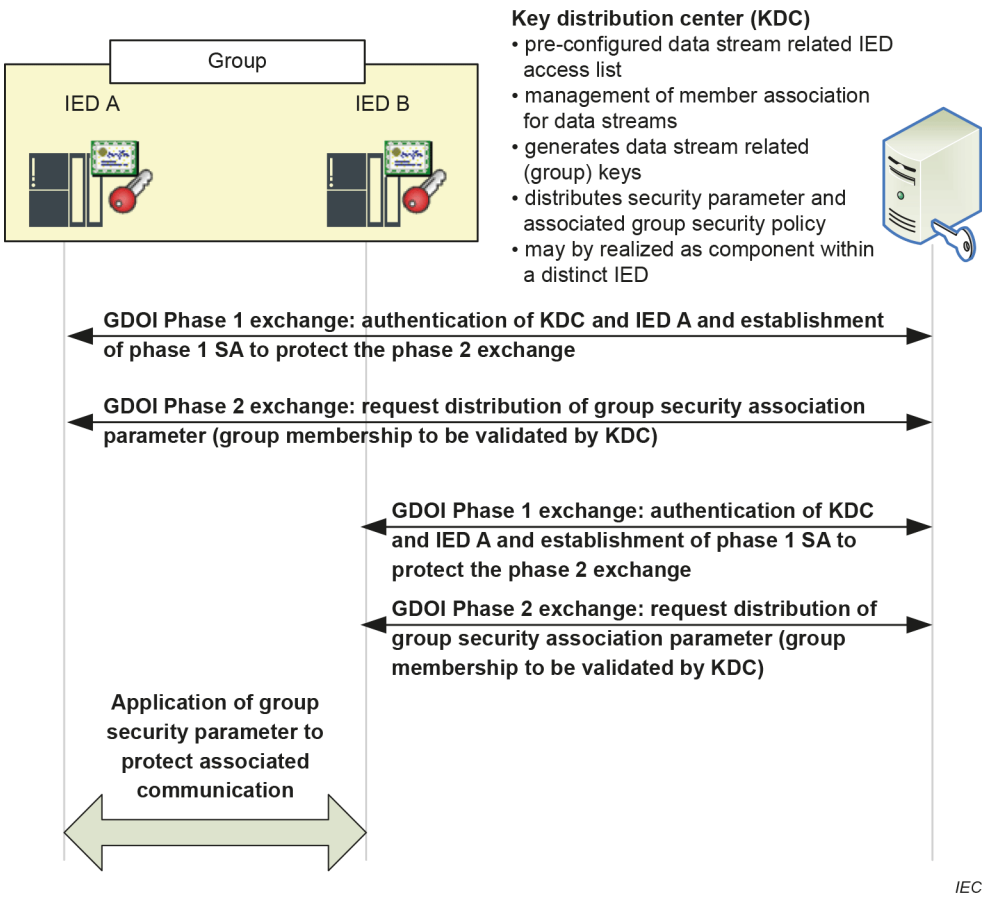


**Figure 3 – Overview of group key management on the example of GDOI**

Figure 3 shows the subscription of an Intelligent Electronic Device (IED) for the security parameters of a data stream. The data stream is associated with a communication group. Note that the group controller may be a separate entity or may be deployed within any IED. Note also that the version shown uses a certificate-based authentication, employing digital signatures.

There exist a number of different protocols for distributing group keys. However, Group Domain of Interpretation (GDOI) has been selected as the most appropriate protocol for power system automation and is further described in5.6.4.2.

AVA Documents
Document Sharing Hub

#### 5.6.4.2 Group Domain of Interpretation (GDOI)

##### 5.6.4.2.1 General

The Group Domain Of Interpretation (GDOI) defined in RFC 6407 supports the distribution of symmetric group keys (i.e., Traffic Encryption Key, TEK) to all pre-configured or otherwise enrolled entities, typically devices. This method requires a Key Distribution Centre (KDC) that is responsible for distributing symmetric session key sets to enrolled entities following the GDOI process. This process uses point-to-point communications between the KDC and each group member (GM) to distribute the symmetric group keys and the associated security policy. The group key itself is then applied according to the provided security policy to protect subsequent communications within the group.

Note that a KDC failure will disrupt group communication, so KDC redundancy is imperative. However, the method for achieving KDC redundancy is outside the scope of this document.

GDOI is specified to proceed in two phases, which are described in more detail in the following sub clauses.

##### 5.6.4.2.2 GDOI Phase 1: Internet Key Exchange (IKE) Phase 1

The GDOI Phase 1 security association provides mutual authentication and authorization. The result is used by the protocol participants to execute a secured GDOI Phase 2 exchange. The GDOI RFC incorporates (i.e., uses but does not redefine) the IKEv1 Phase 1 security association definition from the Internet DOI [RFC2407], [RFC2409] as shown in Figure 4. The symmetric key transfer from the KDC to the entities is initiated after mutual authentication.

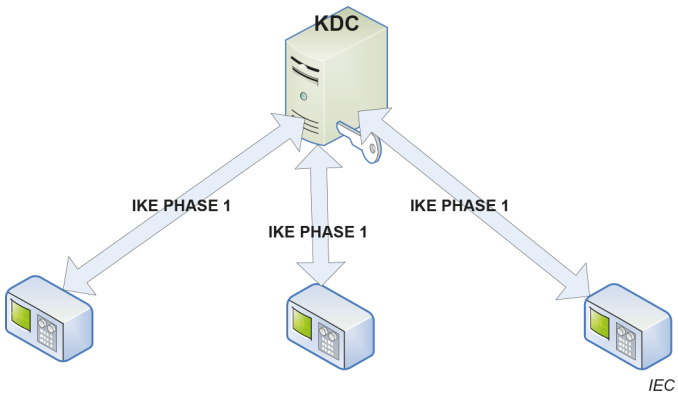


**Figure 4 – GDOI IKE Phase 1 – Authentication and securing communication channel**

NOTE Although RFCs 2407, 2408, and 2409 were obsoleted by RFC 4306 (and subsequently [RFC 5996]), they are used by GDOI because the protocol definitions remain relevant for ISAKMP protocols other than IKEv2.

##### 5.6.4.2.3 GDOI Phase 2: GDOI symmetric key distribution

###### 5.6.4.2.3.1 General

In the GDOI process (RFC 6407), two methods are defined on how to transfer the keys from the KDC into the entities. The first method is the PULL Method (keys are pulled by the entities from the KDC) and the second is the PUSH Method (the keys are pushed from the KDC into the entities) model. The GDOI phase 2 exchange is protected with the SA established in the GDOI phase 1.

NOTE The PUSH Method requires that the group members are reachable from the KDC directly. This has to be obeyed when designing the system architecture as firewalls or NAT devices may hinder this communication.

Either a GROUPKEY-PULL exchange or GROUPKEY-PUSH exchange may be used to distribute symmetric keys to the entities. GROUPKEY-PULL is required to be supported in

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

GDOI, as it is the only method that works in conjunction with the Phase 1 authentication and authorization. There are advantages associated with each of the two methods. GROUPKEY-PULL offers control over traffic delivery while GROUPKEY-PUSH allows for a timely revocation or eviction of an entity and better efficiency.

GDOI has been extended to support IEC 62351 Security Services within RFC 8052. These are described in 5.6.4.2.4.

#### 5.6.4.2.3.2 GROUPKEY-PULL registration protocol exchange

The GDOI Pull Method is illustrated in Figure 5.

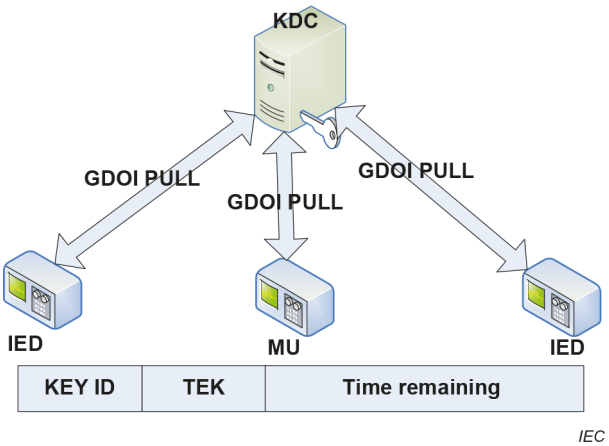


**Figure 5 – GDOI Pull Phase 2**

There are two phases of communication in the GDOI GROUPKEY-PULL method:

- GDOI Phase 1: Connection establishment and authentication of the two participating entities, a group member and KDC as described in 5.6.4.2.2.
- GDOI Phase 2: Determining the policies in use for the requesting group and downloading the keys: This is accomplished through a Group Member (GM) making a GDOI Identification Payload Request to the KDC. The KDC responds to this request with the policies (e.g., encryption and signature algorithms) that are supported. The policies are returned using GDOI SA, which returns a SA TEK payload. If the GM does not support the policies, the communications should abort. If the GM can support the policies, it issues an acknowledgement and the KDC replies with the Key Download (KD) payload.

#### 5.6.4.2.3.3 GROUPKEY-PUSH rekey protocol exchange

The KDC policy may include the use of the "push" method for rekeying, in which case a datagram initiated ("pushed") by the KDC is delivered to all group members using an IP multicast address or is sent to a specific GM using IP unicast. The GROUPKEY-PUSH method is useful for evicting group members that may have been compromised and may have had their certificates revoked. Using this method, the KDC can rekey all authorized group members while excluding the group member that is being evicted.

In case of using GROUPKEY-PUSH, RFC 8263 defines the provisioning of an acknowledgement message from the group members to inform the KDC about the reception of the pushed information. The request to provide the acknowledgement message is indicated by the KDC in the associated policy send to the group members.

#### 5.6.4.2.4 GDOI protocol support for IEC 62351 security services

RFC 8052 "GDOI Protocol Support for IEC 62351 Security Services" was developed to address the use of GDOI for the IEC 61850 power utility automation family of standards. It describes the

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

methods to be used to distribute security transforms that are used for the protection of messages for some IEC 61850-related security protocols: the protection of the messages is defined within IEC 62351-6 [IEC-62351-6], IEC 61850-8-1 [IEC-61850-8-1], and IEC 61850-9-2 [IEC-61850-9-2]. Protected IEC 61850 messages typically include the output of a Message Authentication Code (MAC) and may be encrypted using a symmetric cipher such as the Advanced Encryption Standard (AES).

## 5.7 Trust supported by public-key infrastructures (PKI) and privilege management infrastructures (PMI)

### 5.7.1 General

This clause provides an overview about the PKI infrastructure utilized to manage certificates through the lifecycle of the power system entities (see Figure 6). Note that entities may be devices, systems, but also human users in a power system.

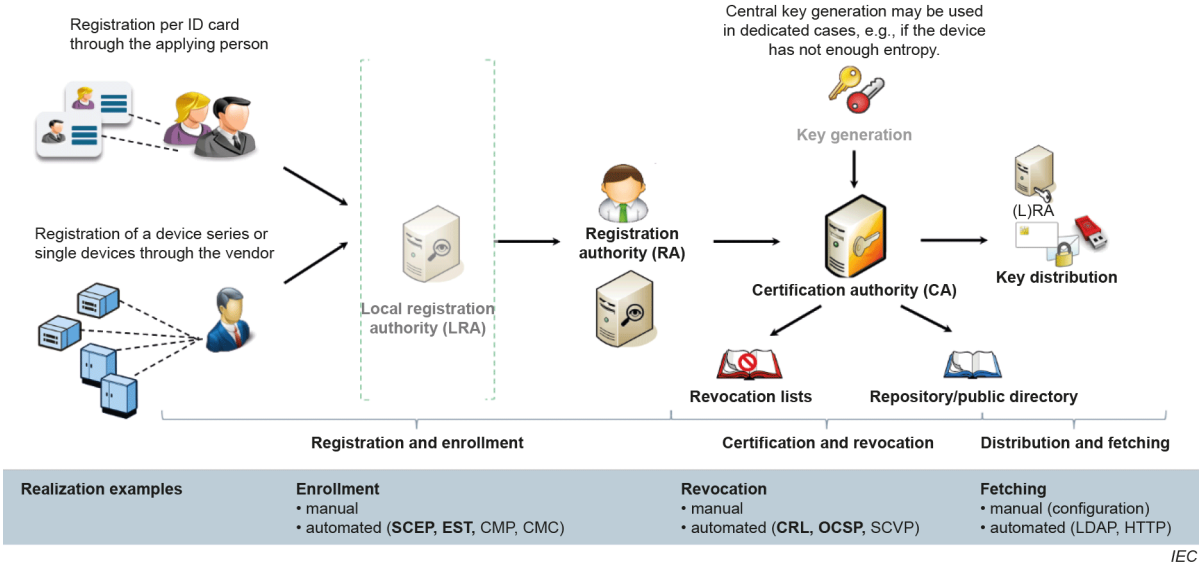


**Figure 6 – Overview of PKI infrastructure and realization examples**

Subclauses 5.7.2 to 5.7.6 describe the general functionality of the registration authority and the certification authority as well as the certificates as managed objects.

### 5.7.2 Registration authorities (RA)

In PKI-based systems, entities are required first to prove their identity through a Registration Authority (RA). For humans, RAs may determine an individual identity through birth certificates, passports, or other official documents. For systems and devices, RAs may determine an entity's identity through a manufacturer-issued digital certificate or a unique one-time-password (OTP).

The RA may either be a separate entity, or it may be part of certification authority (CA).

### 5.7.3 Certification authority (CA)

After its identity is established, a system or device needs to be bound to a certificate by a certification authority (CA). The CSR containing the public key of the generated key pair is either generated by the entity itself or by the manufacturer if the entity is not capable of key generation, e.g., due to missing entropy.. The CA verifies the CSR and issues a digital certificate based on the data included in the CSR. With the certificate, CAs establish a trusted cryptographic binding between the entity's public key and the public-key certificate component data (i.e. the CA's digital signature computed on the combination of the public key and metadata). This public-key certificate thus binds the entity's identity with its public key, so that there is now a trusted public/private key combination that can be used by the entity to exchange

AVA Documents Document Sharing Hub

information with other entities. The trust in the entity's key thus relies on one's trust in the validity of the CA's key (see 5.7.4).

CAs may be operated either by an organization itself, allowing for a closed, organization-controlled communication group, or by a third party (service provider, system operator or grid manager) that is publicly accepted and hence has a wider scope of trust. Third-party CAs require a secure method for accepting the identity of any new entity, which can range from in-person validation for humans to business-entity validation and to security chains of public-key certificates linking previously validated public-key certificates to new public-key certificates.

### 5.7.4 Public-key certificates

#### 5.7.4.1 General

A public-key certificate is a digital document that cryptographically binds the identity of an entity to a public-key of that entity. The public key has a corresponding private key. As noted in 5.7.3, this binding is verified by a digital signature by the issuing CA. In addition to the public key and identity of the owner of a public-key certificate, the public-key certificate holds verified information about validity period and the identity of the issuer. A public-key certificate may include extensions providing additional information. An extension is identified by an object identifier allocated by the organization defining the extension. A public-key certificate may be issued to a CA and is then called a CA certificate or to an end entity and is then called an end-entity public-key certificate.

In a PKI environment, public-key certificates may be digitally signed by the CA of the organization to which the entity belongs. In some cases, multiple public-key certificates are created as an entity goes through a supply chain from manufacturer, to distributer, to purchaser, to installer, etc. Root certificates of the issuing CA become the trust anchors, if used. Typically, organizations should install only CA certificates from CAs they trust, including public-key certificates issued by their own CA.

Public-key certificates may be assigned to entities like devices or human users or software applications.

Public-key certificates are defined by a base set plus extensions to the base set. Extensions are identified by object identifiers.

#### 5.7.4.2 Short-lived public-key certificates

Short-lived certificates (public-key certificates or attribute certificates) may not need to be revoked, as the possibility for compromise is quite low. Short-lived public-key certificates are probably not very useful for the power industry, as they may imply additional overhead for issuing and distributing new public-key certificates, but there may be special circumstances where they could be used.

#### 5.7.4.3 Public-key certificate renewal

When certificates are ready to expire, entities need to apply for certificate renewal using a similar process to enrolment, but simpler since the certificate update can already utilize the available certificate information.

Typically, existing enrolment protocols allow the re-enrolment utilizing the previously issued certificate. The specific process implemented depends on the security policy of the operator.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

#### 5.7.4.4 Alternative process for asymmetric keys generated outside the entity

Asymmetric key pairs may be generated externally if the entity lacks good random number generation capabilities or the necessary computational power. In that case, the generation process may be delegated to a PKI compliant component, such as a PKI tool. Distribution of the keys would need to be done out-of-band using a trusted procedure. The private key may be protected with a transport key as in PEM, PKCS #8 or usually PKCS #12 which may include other objects, such as CA or root certificates. Figure 7 shows one possible option to realize centralized key and certificate generation. The distribution of the key material may be done by using a PKI tool locally.

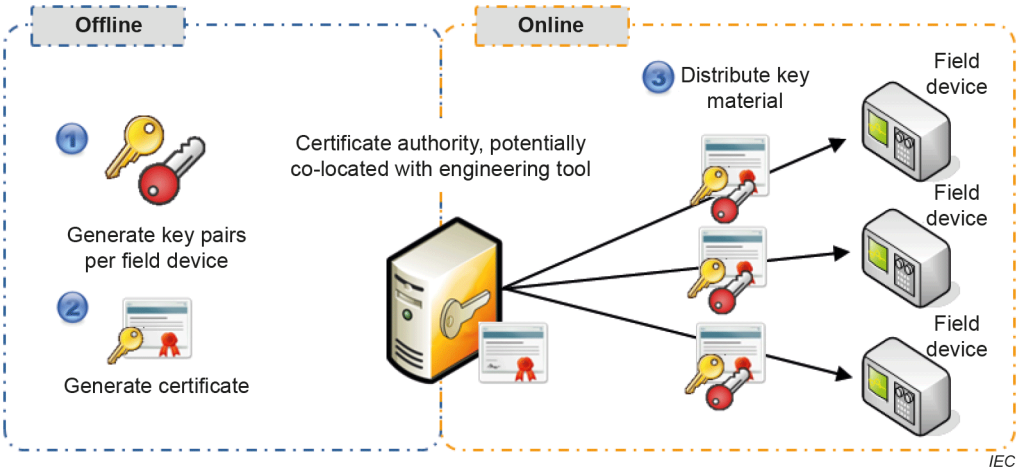


**Figure 7 – Central certificate generation**

If a manufacturer-based credential is already available in the field entity and is trusted by the infrastructure (issuing CA in the new deployment domain), this credential may be used to identify the field entity and to secure the key distribution operation. This requires that the credential be already known at the CA.

### 5.7.5 Attribute certificates

Attribute certificates provide an effective way to separate the management of identity from the management of authorizations associated with an identity. Full separation can be achieved by managing public-key certificates with a PKI and attribute certificates with a "privilege management infrastructure" (which uses the same CA technology as a PKI).

As shown in Figure 8, attribute certificates can be used to extend the information in a public-key certificate. They allow for instance for temporary enhancement of the permissions of the public-key certificate holder by specific role-based access information. This approach has been leveraged in IEC 62351-8.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

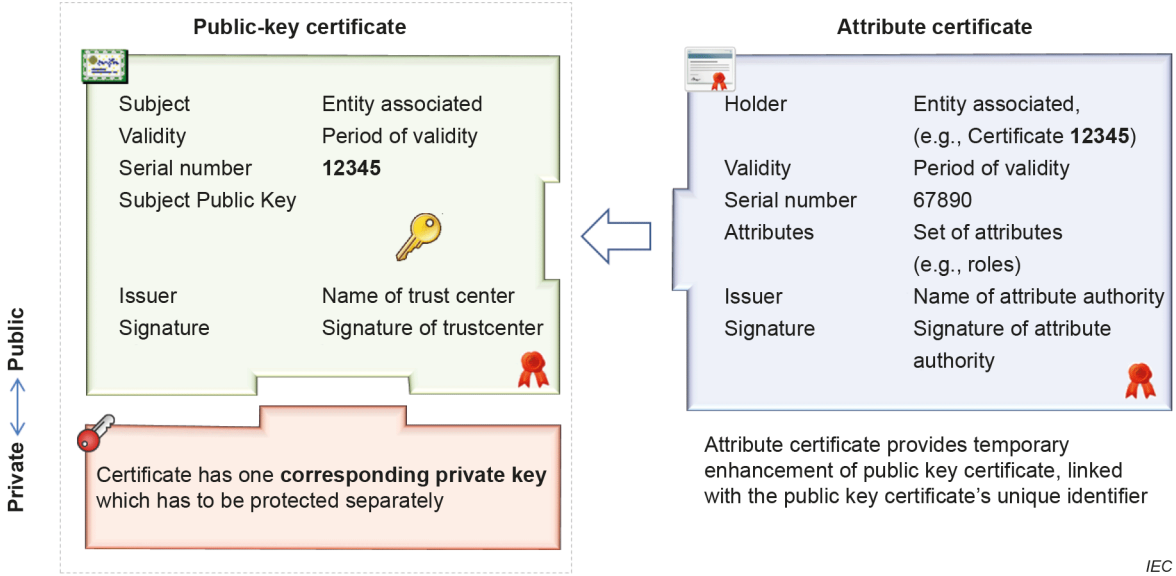


**Figure 8 – Relationship between public-key certificates and attribute certificates**

Attribute certificates may be assigned to entities like devices or human users or software applications.

Attribute certificates are defined by a base set plus extensions to the base set. Extensions are identified by object identifiers.

Attribute certificates can be seen as another approach to achieve a short-lived or temporal extension to a public-key certificate (see also 5.7.4.2). Short-lived attribute certificates can be applied to temporarily extend the permissions of an entity as defined in IEC 62351-8, e.g., for RBAC in general and in emergency cases. Such an attribute certificate should include the no revocation information extension defined in ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019).

### 5.7.6 Public-key certificate and attribute certificate extensions

Both public-key certificates and attribute certificates allow extensions to be optionally included. Each such extension provides additional information.

An extension type consists of an object identifier (see 7.6) that identifies the type of extension and specifies the syntax for the associated information. In addition, it includes a Boolean that specifies whether a particular extension is flagged as critical or as non-critical. If an extension is flagged as critical, it cannot be ignored, and the public-key or attribute certificate is considered invalid if the relying party does not support the type of extension. If the extension is flagged as non-critical, the relying party may ignore the extension if the extension type is not supported. For more details, see 7.3 of ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019).

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) specifies several general applicable extensions. IEC 62351-8 specifies the `IECUserRoles` extension, which has been defined for power systems to provide means for role-based access control.

## 5.8 Certificate management of public-key certificates

### 5.8.1 Certificate management process

The certificate management process may be repeated upon certificate creation, each change of ownership or use of the entity, and when the certificate is about to expire.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

Beyond the utilized mechanisms and protocols used for certificate management, which are detailed in the following sub clauses, two important properties are to be obeyed in the certificate management process with respect to the requester:

- Proof of identity, to ensure that the right entity is considered in the certificate management. This can be done by using different means, such as device-related information together with an activation code (OTP) or an already available certificate and corresponding private key. Specifically, the latter allows for a higher degree of automation of the process.
- Proof of possession of the corresponding private key, to ensure that the provider of the public key also owns the private key. This is typically done by digitally signing the request information (e.g., a PKCS #10 certification request), which can be verified by the central registration authority.

To request a certificate a combination of both, proof of identity and proof of possession is required, to ensure that for the intended entity a public-key certificate will be issued in an authorized way.

### 5.8.2 Initial certificate creation

Just as a birth certificate is the proof of the identity of a person and the physical presence of that person at a registration office is required for personal identification, a device or system needs to have proof of its identity, usually when it is still on the manufacturer's premises and when received by the new owner. This is achieved by registering it with a RA and issuing a certificate by the CA of the manufacturer. This certificate can be verified against the trust anchor of that manufacturer, which therefore needs to be publicly available. Registration could be manual for individual entities or could be handled in bulk for large numbers of entities. The registration process then acts as the source of the supply chain trust or provenance of the entity.

In the context of IEEE 802.1AR, the initial credential is called IDevID for initial device identity. It is a triplet, which consists of the initial device certificate, the corresponding private key, and the certificate chain up to the trust anchor of the issuer (here the manufacturer).

### 5.8.3 Onboarding of an entity

Introducing an entity into a network requires a mutual trust establishment between the entity and the operational domain, typically resulting in the device possessing the trust anchor of the operational domain and also their own certificate and corresponding private key to authenticate other components of the same domain. Here, a similar triplet is built as for the initial device credential by having an operational credential. IEEE 802.1AR references this operational credential as LDevID for locally significant device identifier, consisting of the local device certificate, the corresponding private key, and the certificate chain to a root certificate of the local issuer. Note that a device may possess multiple LDevIDs for different purposes.

The onboarding can be a fully manual process by providing the delivery information of the vendor to the domain for further verification on the infrastructure side. Part of this is the configuring of the domain trust information into the device. This provides the necessary boundary condition for the enrolment as the next step. The latter part, establishing the trust from the entity into the operational domain, can also be automated, resulting in a zero-touch onboarding from a device perspective. To support this automation, information objects and interaction protocols defined by the IETF in the context of autonomous networking can be leveraged. Note that the following examples do not constitute a complete list of possible approaches.

RFC 8366 [44] specifies a voucher artefact that can be used to convey information (the domain certificate of the new owner) from the manufacturer to a device in a protected (signed) container. This signature can be validated by the device requiring the device to possess the root certificate of the manufacturer. Here the assumption is that the devices are shipped with an IDevID.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

RFC 8572 [76] defines a mechanism to securely provision a networking device when it is booting in a factory-default state (Secure Zero Touch Provisioning, SZTP). It may be used in public or private networks and builds on the voucher as defined in RFC 8366 to facilitate trust establishment and also the enrolment of operational certificates for the domain. After finalization of the bootstrapping, the device is able to establish secure connections with other systems.

RFC 8995 [47] builds on the defined voucher process and defines an architecture and protocol (Bootstrapping of remote secure key infrastructures, BRSKI) to establish mutual trust by providing a new device with the local domain certificate information by involving the manufacturer issuing a voucher including this domain certificate. This voucher can be verified by the device as it possesses the trust anchor from the manufacturer. Once the device possesses the domain certificate, it can enrol in the target domain and receive an LDevID (local device identifier) certificate for the new domain. The LDevID is also a triplet, which consists of the local device certificate, the corresponding private key, and the certificate chain to a trust anchor of the issuer (here the operator of the target domain). Utilizing the bootstrapped information for the network level LDevID the device may be provided with further application specific LDevIDs to establish secure communication connections with other devices.

In addition, RFC 8520 [46] (Manufacturer Usage Description, MUD) defines a further approach of supporting automation when installing new devices by specifying information objects to be used by a manufacturer to provide information about the device itself as well as the communication behaviour / expectations of the device. The latter can be used to adopt the infrastructure to the communication needs according to the local security policy. This information may be used, for instance, to refine access control lists in the infrastructure or communication ports with respect to external services. As a result, MUD enables network segmentation by using fine-granular access control definitions based on the purpose and capabilities of the device.

### 5.8.4 Enrolment of an entity

Enrolment is the process by which the entity receives a signed certificate from the CA in the operational environment. Based on the existing security credentials of the entity, different enrolment scenarios can be distinguished:

- One-time unique password without certificate
- With CA-issued certificate (this may be an IDevID issued by a manufacturer CA)
- With known (authorized) self-signed certificate
- With expired or revoked certificate (this may be an IDevID issued by a manufacturer CA or an LDevID from a local CA)
- With an expired or revoked CA certificate.

There exist different protocols for enrolment and management of certificates that support different sets of functionalities. Four of them are briefly described in 5.8.6. Of these, two are focused on the applications used in the power system domain, which are SCEP (see 5.8.6.1) and EST (see 5.8.6.2). Both protocols address the main functionality seen as necessary to manage certificates from devices in a power system, while keeping simplicity, and both provide a subset of the functionality provided by the rather feature rich protocols CMP (see 5.8.6.3) and CMC (see 5.8.6.4). These latter two enrolment protocols provide better support in offline scenarios and in support of revocation handling.

An example of enrolling an entity using SCEP is shown in Figure 9. For SCEP, the activation code is an OTP (One-Time-Password) as illustrated in Figure 9 or an existing certificate. For EST, the activation code may a username and a password or an existing key pair (e.g., a manufacturer issued (imprinted) certificate with a corresponding private key and issuing CA information, IDevID).

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-9:2023

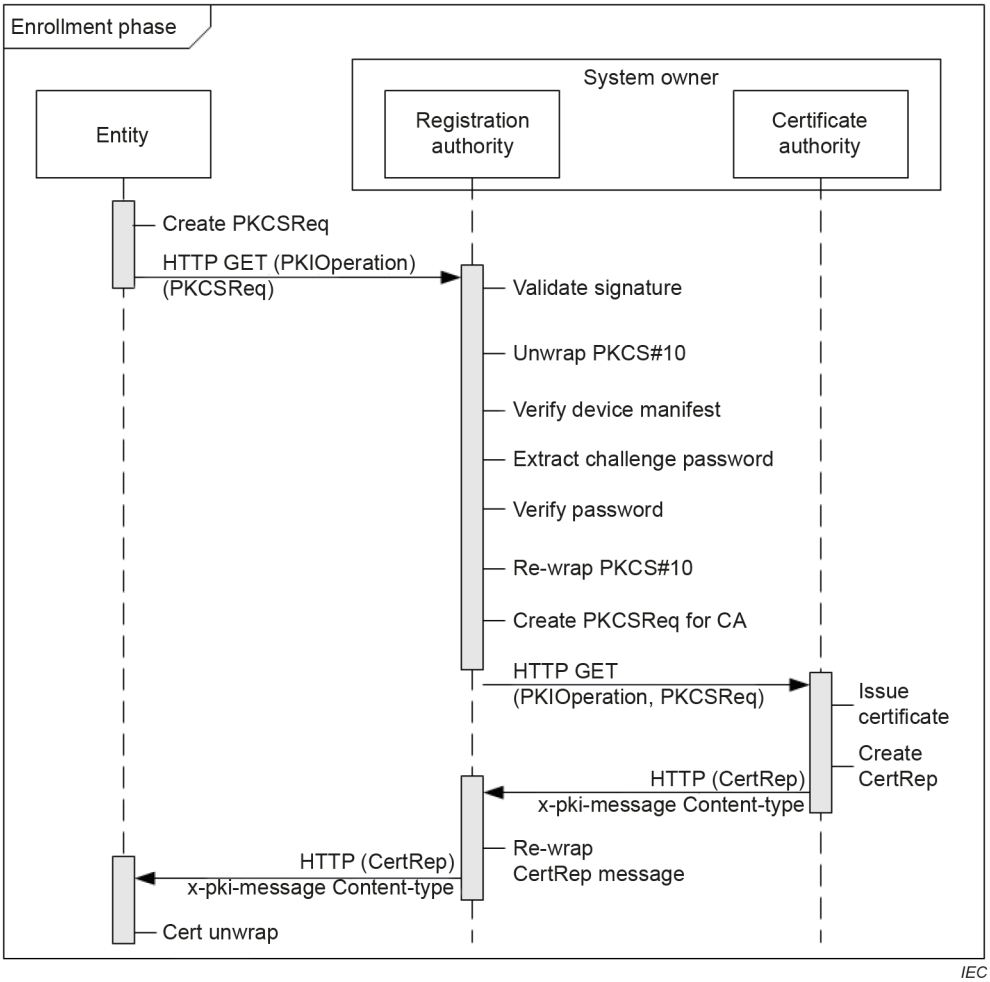


**Figure 9 – Example of the SCEP entity enrolment and CSR process**

An example of enrolling an entity using EST is shown in Figure 10.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

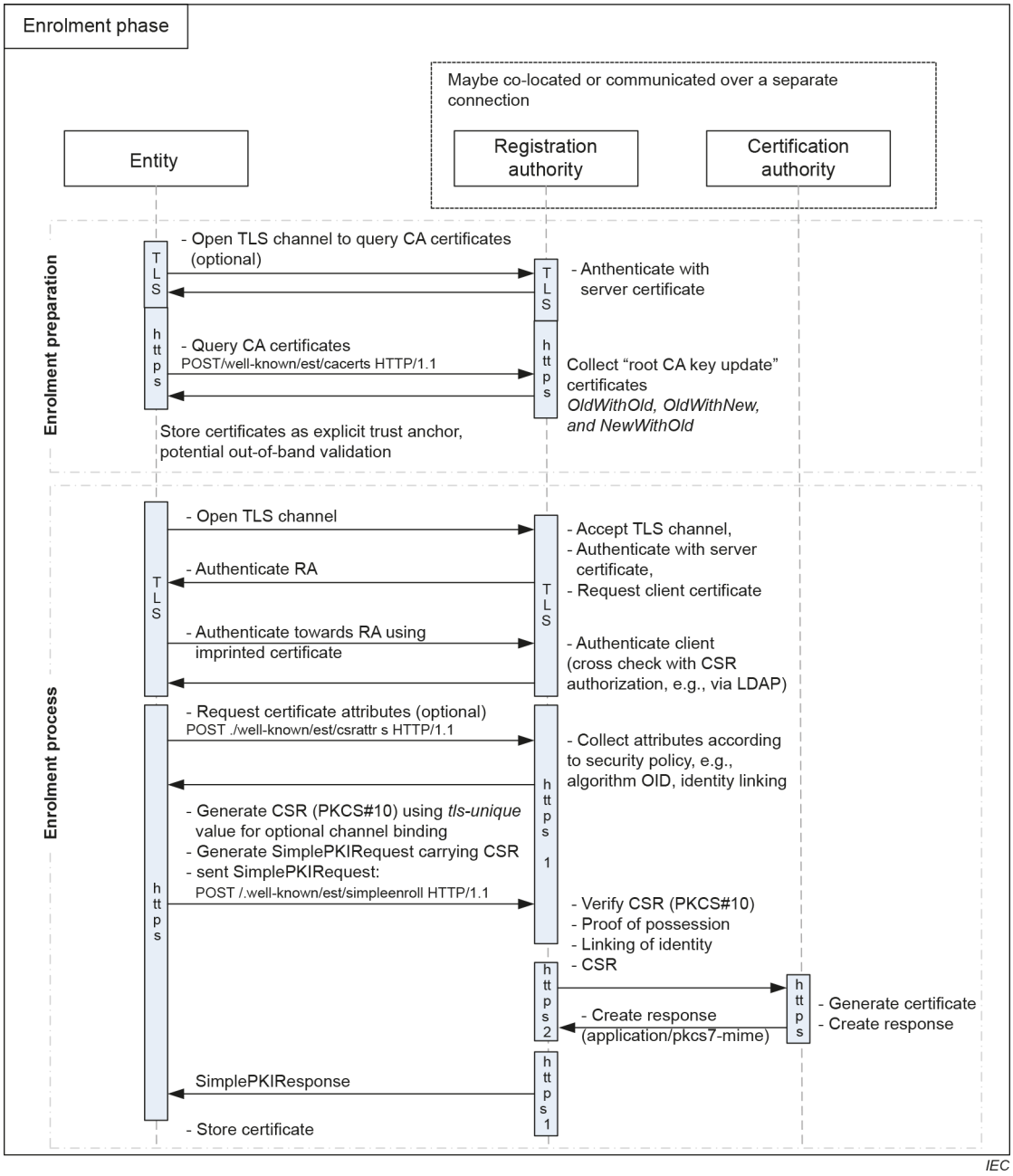


**Figure 10 – Example of the EST entity enrolment and CSR process**

Notes about Figure 9 and Figure 10:

- Prior to enrolment, devices must be configured. Besides their standard configuration, such as their own IP address(es), they must also be given their PKI enrolment data, RA/CA IP address, trust anchor certificates (CA/Root certificate), etc. As stated in 5.8.3, this process can be manual or automated. Automated provisioning can be supported by example protocols stated in 5.8.3.
- The entity checks the authenticity of communication peers based on the root certificate of the CA. This root certificate is fed to the device during the device configuration phase (see 7.3.6) or as part of an automated onboarding. The CA signs the certificates issued with the CA private key. Entities check the authenticity of the received certificate by verifying the signature in the certificates using the CA public key.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

### 5.8.5 Certificate signing request (CSR) processing

#### 5.8.5.1 Enrolment process

The enrolment process involves certificate signing by a CA to verify the identity of an entity, to verify that the entity possesses the private key associated with the public key, and to issue a certificate to that effect. This certificate signing requires the entity (device) to issue a certification request to the RA/CA. The CSR processing, using device generated key material, consists of the following steps, as illustrated in Figure 11.

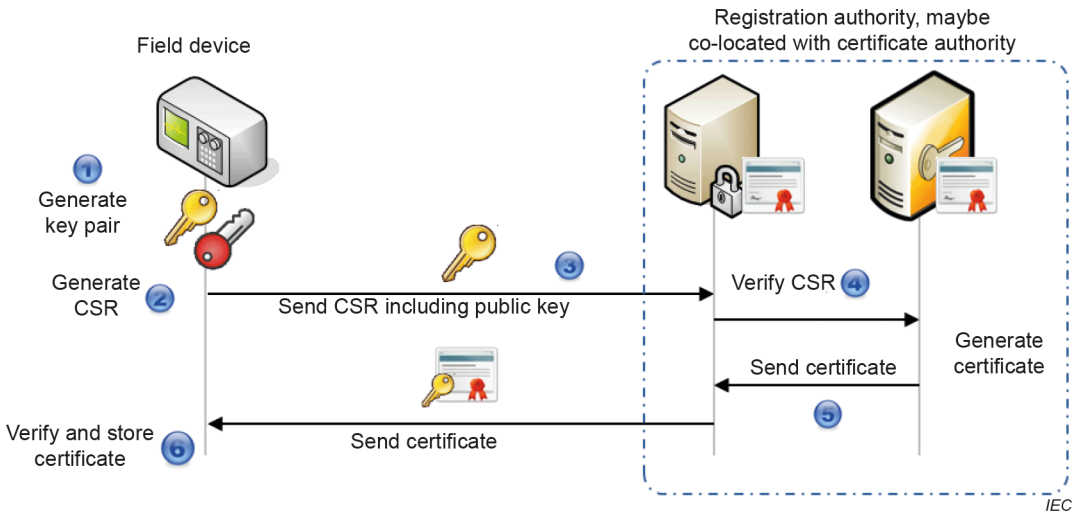


**Figure 11 – CSR processing**

1) The entity generates a pair of public and private keys.
2) The entity generates a *CertificationRequestInfo,* here using the PKCS #10 specification format [18]. This request contains a "subject distinguished name", the public key from the public/private pair it just generated (see ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)), and optionally a set of attributes. The *CertificationRequestInfo* is signed with the entity's private key. The *CertificationRequestInfo*, a signature algorithm identifier, and the entity's signature go into a *CertificationRequest* structure. See [18].
3) The entity sends the *CertificationRequest* message to the RA/CA for authorization and certification as part of an enrolment protocol (see 5.8.6).
4) The RA validates the request by verifying the signature on the incoming request.
5) If the request is valid, the RA authenticates the requesting entity and, if valid and authorized, invokes the CA, which creates a public-key certificate from the distinguished name and public key, the issuer name, and the certification authority's choice of serial number, validity period, optional extensions and digital signature algorithm providing the information for the signature of the listed data. The CA then sends the certificate via the RA to the entity.
6) The entity performs the signature verification on the received certificate from the CA to ensure that the received certificate is issued and signed by the trusted CA. Note the assumption here is that the trusted CA certificates are distributed and installed in the entity during the commissioning/onboarding/configuration phase. The entity verifies the signature on the received certificate from the operational CA with the help of these trusted CA certificates. If the CA signature is valid, the entity stores the certificate in the implementation-preferable format and appropriate file extension when storage is file-based (e.g., .der, .pem, .cer, .crt, etc).

The CSR process may require human involvement with an administration role to activate, enable or approve the CSR process. This manual support may be necessary at the same time as the CSR application or may take place in advance, depending on the entity authentication procedure. If an entity is authenticated with a vendor-issued credential (IDevID) or with a one-time password, this information can be provided to the RA in advance.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

The following two subclauses describe the certification requests formats PKCS #10 and CRMF.

#### 5.8.5.2 PKCS #10 certification request

The certification request syntax, as defined by IETF RFC 2986 [18], is used by different public-key certificate management protocols to convey a certification request from a client (end entity) to a CA or an entity interfacing to the CA, e.g., an RA or EST server (see RFC 7030).

IETF RFC 2986 does not specify any response format or how a certification request is carried out, but leaves that to a referencing specification.

The certification request is specified as PKCS #10 in RFC 2986 [18]. A certification request is sent from an entity to the registration authority (RA), which may be co-located with the CA or be physically separated.

Figure 12 illustrates the structure of a certification request. It has the following components:

a) The `Version` component indicates the version of the certification request. The version specified by IETF RFC 2986 is version 1 and is indicated by a value '0'.

b) The Subject component specifies the name to be used in the subject component of the requested public-key certificate.

c) The Subject public-key information component specifies the information to be included in the `subjectPublicKeyInfo` component of the requested public-key certificate.

d) The Attributes component holds a set of directory attributes that provides additional information for the generation of the requested public-key certificates.

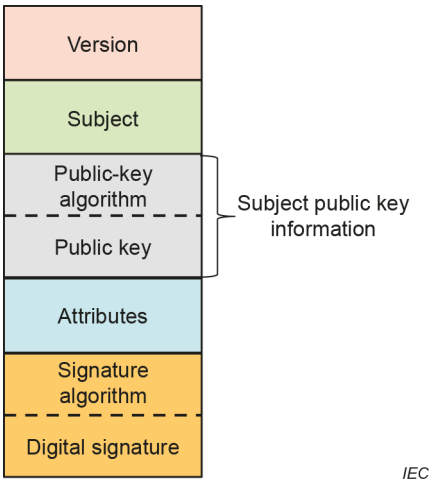


**Figure 12 – Certification request format**

The certification request is digital signed using the private key corresponding to the public key provided in certification request. If the recipient is able to validate the signature using the public key provided in the certification request, it proves that the issuer is in possession of the private key corresponding to the presented public key.

IETF RFC 2985 [19] defines two attribute types considered relevant for inclusion in a certification request:

a) An attribute of the `challengePassword` attribute type may be included and, if present, the same attribute shall be used for a revocation request.

b) An attribute of the `extensionRequest` attribute type may be included and shall then hold a sequence of public-key certificate extensions to be included in the public-key certificates.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023

#### 5.8.5.3 Certificate Request Message Format (CRMF)

The Certificate Request Message Format (CRMF) is specified in IETF RFC 4211 [20] and illustrated in Figure 13.

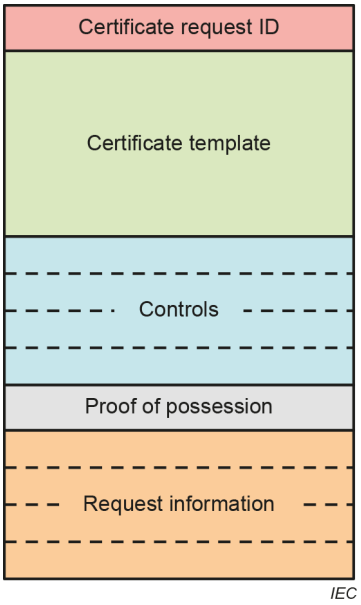


**Figure 13 – Certificate request message format**

Like the certification request described in 5.8.5.2, the CRMF does not constitute a protocol, but is a data type specification to be included in referencing protocol types.

The details of CRMF are found in IETF RFC 4211. An overview of the different parts of CRMF is given in the following:

a) The certificate request ID may be used for pairing requests and responses.

b) The certificate template allows the requestor to specify or omit content for each component of the public-key certificate being requested. It may be a little confusing that specifications for certain components are omitted although the ASN.1 allows their presence. A single component (public-key information) is present, but still listed as optional. For details, see IETF RFC 4211.

c) The controls are attributes that will not to be part of the public-key certificate but provide information about how the context in which the public key is to be issued. IETF RFC 4211 defines a number of controls, like additional authentication information about the subject of the public-key certificate, suggestions on how the public-key certificate is published, suggestions on how the private key should be archived, information about a possible old public-key certificate, and an encryption key to be used by the CA to encrypt the response.

d) The proof-of-possession, when present, provides a detailed specification for how to prove the possession of the private key, depending on whether the key is intended for digital signature encryption (RSA) or for key agreement.

e) The request information

The Certificate Request Message Format (CRMF) syntax and semantics is used to convey a request for a certificate to a CA, possibly via a Registration Authority (RA), for the purposes of public-key certificate production. The request will typically include a public key and the associated registration information.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-9:2023