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

Part 4: Profiles including MMS and derivatives

Documents
Document Sharing Hub

# National foreword

This British Standard is the UK implementation of EN IEC 62351-4:2018+A1:2020. It is identical to IEC 62351-4:2018, incorporating amendment 1:2020. It supersedes BS EN IEC 62351-4:2018, which is withdrawn.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.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 05730 0

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 January 2019.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|
| 31 October 2020 | Implementation of IEC amendment 1:2020 with CENELEC endorsement A1:2020 |

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN IEC 62351-4:2018+A1

September 2020

ICS 33.200

English Version

# Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives (IEC 62351-4:2018)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 4 : Profils comprenant MMS (IEC 62351-4:2018)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 4: Profile einschließlich MMS und Ableitungen (IEC 62351-4:2018)

This European Standard was approved by CENELEC on 2018-12-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

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

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.



AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

## European foreword

The text of document 57/2032/FDIS, future edition 1 of IEC 62351-4, 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 62351-4:2018.

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) 2019-09-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-12-20

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.

## Endorsement notice

The text of the International Standard IEC 62351-4:2018 was approved by CENELEC as a European Standard without any modification.

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

| | | |
|---|---|---|
| IEC 60870-6-503:2014 | NOTE | Harmonized as EN 60870-6-503:2014 (not modified) |
| IEC 60870-6-702:2014 | NOTE | Harmonized as EN 60870-6-702:2014 (not modified) |
| IEC 60870-6-802:2014 | NOTE | Harmonized as EN 60870-6-802:2014 (not modified) |

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

## Foreword to amendment A1

The text of document 57/2217/FDIS, future IEC 62351-4/A1, 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 62351-4:2018/A1:2020.

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) 2021-05-21
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-08-21

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.

## Endorsement notice

The text of the International Standard IEC 62351-4:2018/A1:2020 was approved by CENELEC as a European Standard without any modification.

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

| | | |
|---|---|---|
| IEC 61850-8-1:2011 | NOTE | Harmonized as EN 61850-8-1:2011 (not modified) |
| IEC 61850-8-2:2018 | NOTE | Harmonized as EN IEC 61850-8-2:2019 (not modified) |

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

# 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.cenelec.eu.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC/TS 62351-1 | - | Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues | - | - |
| IEC/TS 62351-2 | - | Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms | - | - |
| IEC 62351-3 | 2014 | Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP | EN 62351-3 | 2014 |
| +A1 | 2018 | | +A1 | 2018 |
| IEC/TS 62351-8 | 2011 | Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control | - | - |
| IEC 62351-9 | 2017 | Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment | EN 62351-9 | 2017 |
| ISO/IEC 8073 | 1997 | Information technology - Open Systems Interconnection - Protocol for providing the connection-mode transport service | - | - |
| ISO/IEC 8823-1 | 1994 | Information technology - Open Systems Interconnection - Connection-oriented presentation protocol: Protocol specification | - | - |
| ISO/IEC 8824-1 | - | Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation | - | - |

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

| | | | | |
|---|---|---|---|---|
| ISO/IEC 8825-1 | - | Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) | - | - |
| ISO/IEC 8825-4 | - | Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) | - | - |
| ISO 8601 | 2004 | Data elements and interchange formats - Information interchange - Representation of dates and times | - | - |
| ISO 9506-2 | 2003 | Industrial automation systems - Manufacturing Message Specification - Part 2: Protocol specification | - | - |
| ITU-T X.509 | - | Information technology - Open Systems interconnection - The Directory: Public-key and attribute certificate frameworks | - | - |
| ITU-T Recommendation X.227 | - | Information technology - Open Systems Interconnection - Connection-oriented protocol for the Association Control Service Element: Protocol specification | - | - |
| + A1 | - | | - | - |
| IETF RFC 1006 | 1987 | ISO Transport Service on top of the TCP, Version: 3 | - | - |
| IETF RFC 2104 | 1997 | HMAC: Keyed-Hashing for Message Authentication | - | - |
| IETF RFC 3526 | 2003 | More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) | - | - |
| IETF RFC 5114 | 2003 | Additional Diffie-Hellman Groups for Use with IETF Standards | - | - |
| IETF RFC 5246 | 2008 | The Transport Layer Security (TLS) Protocol Version 1.2 | - | - |
| IETF RFC 5480 | 2009 | Elliptic Curve Cryptography Subject Public Key Information | - | - |
| IETF RFC 5639 | 2010 | Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation | - | - |
| IETF RFC 5869 | 2010 | HMAC-based Extract-and-Expand Key Derivation Function | - | - |
| IETF RFC 6120 | 2011 | Extensible Messaging and Presence Protocol (XMPP): Core | - | - |
| IETF RFC 6122 | 2011 | Extensible Messaging and Presence Protocol (XMPP): Address Format | - | - |

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

*This page deliberately left blank*

Documents
Document Sharing Hub

# CONTENTS

FOREWORD ..... 8
1 Scope ..... 10
1.1 General ..... 10
1.2 Code components ..... 11
2 Normative references ..... 11
3 Terms, definitions and abbreviated terms ..... 12
3.1 General ..... 12
3.2 Terms and definitions ..... 13
3.3 Abbreviated terms ..... 16
4 Security issues addressed by this part of IEC 62351 ..... 18
4.1 Communications reference models ..... 18
4.2 Security for application and transport profiles ..... 18
4.3 Compatibility and native modes ..... 19
4.4 Security threats countered ..... 19
4.4.1 General ..... 19
4.4.2 Threats countered in compatibility mode ..... 20
4.4.3 Threats countered in native mode ..... 20
4.5 Attack methods countered ..... 20
4.5.1 General ..... 20
4.5.2 Attacks countered in compatibility mode ..... 20
4.5.3 Attacks countered in native mode ..... 20
4.6 Logging ..... 21
5 Specific requirements ..... 21
5.1 Specific requirements for ICCP/IEC 60870-6-x communication stack ..... 21
5.2 Specific requirements for IEC 61850 ..... 22
6 Transport Security ..... 22
6.1 General ..... 22
6.2 Application of transport layer security (TLS) ..... 22
6.2.1 General ..... 22
6.2.2 The TLS cipher suite concept ..... 23
6.2.3 TLS session resumption ..... 23
6.2.4 TLS session renegotiation ..... 23
6.2.5 Supported number of trust anchors ..... 23
6.2.6 Public-key certificate size ..... 23
6.2.7 Evaluation period for revocation state of public-key certificates ..... 23
6.2.8 Public-key certificate validation ..... 24
6.2.9 Security events handling ..... 24
6.3 T-security in an OSI operational environment ..... 24
6.3.1 General ..... 24
6.3.2 TCP ports ..... 24
6.3.3 Disabling of TLS ..... 25
6.3.4 TLS cipher suites support ..... 25
6.4 T-security in an XMPP operational environment ..... 27
7 Application layer security overview (informative) ..... 27
7.1 General ..... 27
7.2 Description techniques ..... 28



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

7.2.1 General ..... 28
7.2.2 ASN.1 as an XML schema definition ..... 28
7.2.3 W3C XML Schema Definition (W3C XSD) ..... 28
7.2.4 XML namespace ..... 29
8 Use of cryptographic algorithms ..... 29
8.1 General ..... 29
8.2 Basic cryptographic definitions ..... 29
8.3 Public-key algorithms ..... 30
8.4 Hash algorithms ..... 30
8.5 Signature algorithms ..... 30
8.6 Symmetric key algorithms ..... 31
8.7 Authenticated encryption algorithms ..... 31
8.8 Integrity check value algorithms ..... 32
9 Object identifier allocation (normative) ..... 32
10 General OSI upper layer requirements (normative) ..... 33
10.1 Overview ..... 33
10.2 General on OSI upper layer requirements ..... 34
10.3 Session protocol requirements ..... 34
10.4 Presentation protocol requirements ..... 34
10.4.1 Context list ..... 34
10.4.2 Abstract syntaxes ..... 35
10.4.3 Presentation user data ..... 35
10.4.4 ASN.1 encoding requirements ..... 36
10.5 Association control service element (ACSE) protocol requirements ..... 36
10.5.1 General ..... 36
10.5.2 Protocol version ..... 36
10.5.3 Titles ..... 36
10.5.4 Use of ASN.1 EXTERNAL data type ..... 37
11 A-security profile (normative) ..... 37
11.1 OSI requirements specific to A-security profile ..... 37
11.1.1 General ..... 37
11.1.2 Additional session protocol requirements ..... 38
11.1.3 Additional presentation protocol requirement ..... 38
11.1.4 Additional ACSE requirements ..... 38
11.2 MMS Authentication value ..... 39
11.2.1 General ..... 39
11.2.2 MMS-Authentication value data type ..... 40
11.2.3 Handling of the association request (AARQ-apdu) ..... 40
11.2.4 Handling of the association result (AARE-apdu) ..... 41
12 End-to-end application security model ..... 41
12.1 Introduction and general architecture ..... 41
12.2 Abstract syntax specifications ..... 43
12.2.1 General ..... 43
13 End-to-end application security (normative) ..... 44
13.1 Association management ..... 44
13.1.1 General concept ..... 44
13.1.2 UTC time specification ..... 44
13.1.3 Handshake request ..... 44



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

13.1.4 Handshake accept ..... 45
13.1.5 Association reject by the protected protocol ..... 46
13.1.6 Association reject due to security issues ..... 46
13.1.7 Handshake security abort ..... 47
13.1.8 Data transfer security abort ..... 47
13.1.9 Abort by protected protocol ..... 47
13.1.10 Association release request ..... 48
13.1.11 Association release response ..... 48
13.2 Data transfer phase ..... 49
13.2.1 General ..... 49
13.2.2 Clear data transfer ..... 49
13.2.3 Encrypted data transfer ..... 49
13.3 ClearToken data types ..... 50
13.3.1 The ClearToken1 data type ..... 50
13.3.2 The ClearToken2 data type ..... 55
13.3.3 The ClearToken3 data type ..... 56
13.4 Authentication and integrity specifications ..... 57
13.4.1 The Signature data type ..... 57
13.4.2 The authenticator data type ..... 57
14 E2E security error handling (normative) ..... 57
14.1 General ..... 57
14.2 Specification of diagnostics ..... 57
14.2.1 Handshake diagnostics ..... 57
14.2.2 The data transfer diagnostics ..... 59
14.3 Checking of E2E-security handshake request and accept ..... 60
14.3.1 General ..... 60
14.3.2 Signature checking ..... 60
14.3.3 Protected protocol identity checking ..... 61
14.3.4 ClearToken1 checking ..... 61
14.4 Checking of security protocol control information during data transfer ..... 63
14.4.1 General ..... 63
14.4.2 Authenticator checking ..... 63
14.4.3 Checks of the ClearToken2 value ..... 63
15 E2E security used in an OSI operational environment ..... 64
15.1 General ..... 64
15.2 Additional upper layer requirements ..... 64
15.2.1 Additional presentation layer requirements ..... 64
15.2.2 Additional ACSE requirements ..... 64
15.3 Association management in an OSI operational environment ..... 64
15.3.1 General ..... 64
15.3.2 Mapping to ACSE association request ..... 65
15.3.3 Mapping to ACSE association response ..... 65
15.3.4 Mapping to ACSE abort ..... 66
15.3.5 Mapping to ACSE release request ..... 67
15.3.6 Mapping to ACSE release response ..... 67
15.4 Data transfer in OSI operational environment ..... 67
15.4.1 General ..... 67
15.4.2 Mapping of the clear data transfer SecPDU ..... 67
15.4.3 Mapping of the encrypted data transfer SecPDU ..... 68



AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

15.5 OSI upper layer routing ..... 68
15.6 OSI operational environment checking ..... 70
15.6.1 General checking ..... 70
15.6.2 Environment mapping checking ..... 70
15.6.3 OSI operational environment diagnostics ..... 71
16 E2E security used in in an XMPP operational environment ..... 71
16.1 General on wrapping to an XMPP operational environment ..... 71
16.2 Mapping of SecPDUs to iq stanzas ..... 72
16.3 Mapping of SecPDUs to message stanzas ..... 73
16.4 XMPP stanza error handling ..... 73
16.5 XML namespaces ..... 74
16.6 Encoding of EnvPDUs within XMPP stanzas ..... 74
16.7 Multiple associations ..... 75
16.8 Release collision consideration ..... 75
17 Conformance to this document ..... 75
17.1 General ..... 75
17.2 Notation ..... 75
17.3 Conformance to operational environment ..... 75
17.4 Conformance to modes of operation ..... 76
17.5 Conformance to compatibility mode ..... 76
17.6 Conformance to native mode ..... 76
Annex A (normative) Formal ASN.1 specification for the A-security-profile ..... 79
Annex B (normative) Formal ASN.1 specification for the End-to-End security ..... 80
Annex C (normative) Formal W3C XSD specification for the end-to-end security ..... 85
Annex D (normative) ASN.1 module for OSI operational environment ..... 93
D.1 Scope of annex ..... 93
D.2 ASN.1 module ..... 93
Annex E (normative) ASN.1 modules and W3C XSDs for an XMPP operational environment ..... 95
E.1 Scope of Annex ..... 95
E.2 ASN.1 modules for the XMPP operational environment ..... 95
E.2.1 ASN.1 module for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace ..... 95
E.2.2 ASN.1 module for the http://www.iec.ch/62351/2018/ENV_4 XML namespace ..... 95
E.3 W3C XSDs for the XMPP operational environment ..... 97
E.3.1 W3C XSD for the urn:ietf:params:xml:ns:xmpp-stanzas XML namespace ..... 97
E.3.2 W3C XSD for the http://www.iec.ch/62351/2018/ENV_4 XML namespace ..... 98
Annex F (normative) Template for virtual API specifications ..... 100
F.1 General ..... 100
F.2 ASN.1 virtual API specification ..... 101
F.3 ASN.1 virtual API specification for OSI environment ..... 101
F.4 W3C XSD virtual API specification ..... 101
Annex G (normative) End-entity public-key certificate specification ..... 103
G.1 Scope of annex ..... 103
G.2 General requirement ..... 103
G.3 Length considerations ..... 103
G.4 Basic Structure requirement and recommendations ..... 103



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

G.4.1 Version component ..... 103
G.4.2 Serial number component ..... 103
G.4.3 Issuer signature algorithm component ..... 103
G.4.4 Issuer component ..... 104
G.4.5 Validity component ..... 104
G.4.6 Subject component ..... 104
G.4.7 Subject public key Information component ..... 104
G.4.8 Issuer unique ID and subject unique ID components ..... 105
G.5 Extensions ..... 105
G.5.1 General ..... 105
G.5.2 Key usage extension ..... 105
G.5.3 Revocation checking ..... 105
G.5.4 IEC user role information extension ..... 106
G.6 Specific requirements for operational environments ..... 106
G.6.1 General ..... 106
G.6.2 OSI operational environment ..... 106
G.6.3 XMPP operational environment ..... 106
Annex H (normative) Lower layer requirements for the OSI operational environment ..... 107
H.1 Scope of annex ..... 107
H.2 Transport protocol class 0 ..... 107
H.2.1 Enforcement of maximum lengths ..... 107
H.2.2 Response to Class 0 unsupported TPDUs ..... 107
H.2.3 Transport selectors ..... 107
H.3 IETF RFC 1006 ..... 108
H.3.1 General ..... 108
H.3.2 Version number ..... 108
H.3.3 Length ..... 108
H.3.4 Keep-alive ..... 108
Annex I (informative) ASN.1 definition of ACSE ..... 109
Bibliography ..... 113

Figure 1 – Application and transport profiles (informative) ..... 18
Figure 2 – T-profiles without and with TLS protection ..... 24
Figure 3 – Association establishment ..... 33
Figure 4 – Inclusion of User-data in SESSION DATA TRANFER SPDU ..... 36
Figure 5 – E2E security building blocks ..... 42
Figure 6 – Relationship between environment, E2E-security and protected protocol ..... 42
Figure 7 – Relationships between APDUs ..... 43
Figure 8 – The scope of E2E-security specification ..... 43
Figure 9 – Upper layer routing ..... 69
Figure F.1 – Virtual API concept ..... 100

Table 1 – Relationship between security and security measure combinations ..... 19
Table 2 – Commented recommended cipher suites from IEC TS 62351-4:2007 ..... 26
Table 3 – Cipher suites combinations in the context of this document ..... 27
Table 4 – Mapping of SecPDUs to ACSE **EnvPDUs** ..... 65

AVA Documents
Document Sharing Hub



Full document details: BS EN IEC 62351-4:2018+A1:2020

Table 5 – Mapping of SecPDUs to XMPP stanzas ..... 72
Table 6 – Conformance to operational environment ..... 76
Table 7 – Conformance to modes of operation ..... 76
Table 8 – Conformance to TLS cipher suites in compatibility mode ..... 76
Table 9 – Conformance to mode of encryption ..... 77
Table 10 – Conformance to TLS cipher suites in native mode ..... 77
Table 11 – Conformance to cryptographic algorithms for E2E-security ..... 78
Table H.1 – TP class 0 maximum sizes ..... 107



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

## Part 4: Profiles including MMS and derivatives

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-4 has been prepared by IEC technical committee 57: Power systems management and associated exchange.

The text of this standard is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 57/2032/FDIS | 57/2053/RVD |

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

AVA Documents
Document Sharing Hub



Full document details: BS EN IEC 62351-4:2018+A1:2020

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

This IEC standard includes Code Components i.e. components that are intended to be directly processed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labelled in this standard as a Code Component.

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard to end users either directly or via distributors, subject to IEC software licensing conditions, which can be found at: www.iec.ch/CCv1.

In this document the following print types are used:

– Abstract Syntax Notation One (ASN.1) and W3C XML Schema Definition (W3C XSD) notions are presented in **`bold Courier New`** typeface; and

– when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in **`bold Courier New`** typeface.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

# POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

## Part 4: Profiles including MMS and derivatives

## 1 Scope

### 1.1 General

This part of IEC 62351 extends the scope of IEC TS 62351-4:2007 [1][1] by specifying a compatibility mode that provides interoperation with implementation based on IEC TS 62351-4:2007 and by specifying extended capabilities referred to as native mode.

This part of IEC 62351 specifies security requirements both at the transport layer and at the application layer. While IEC TS 62351-4:2007 primarily provided some limited support at the application layer for authentication during handshake for the Manufacturing Message Specification (MMS) based applications, this document also provides support for extended integrity and authentication both for the handshake phase and for the data transfer phase. It provides for shared key management and data transfer encryption at the application layer and it provides security end-to-end (E2E) with zero or more intermediate entities. While IEC TS 62351-4:2007 only provides support for systems based on the MMS, i.e. systems using an Open Systems Interworking (OSI) protocol stack, this document also provides support for application protocols using other protocol stacks, e.g. an Internet protocol suite (see 4.1). This support is extended to protect application protocols using XML encoding. This extended security at the application layer is referred to as E2E-security.

In addition to E2E security, this part of IEC 62351 also provides mapping to environmental protocols carrying the security related information. Only OSI and XMPP environments are currently considered.

It is intended that this part of IEC 62351 be referenced as a normative part of standards that have a need for using application protocols, e.g., MMS, in a secure manner.

It is anticipated that there are implementations, in particular Inter-Control Centre Communications Protocol (ICCP) implementations that are dependent on the IEC TS 62351-4:2007 specifications of the T-profile and the A-security-profile. The specifications from IEC TS 62351-4:2007 are therefore included in this part of IEC 62351. Implementations supporting these specifications will interwork with implementation based on IEC TS 62351-4:2007.

NOTE The A-security-profile is in the strict sense not a profile, but the term is here kept for historical reasons.

This document represents a set of mandatory and optional security specifications to be implemented to protect application protocols.

The initial audience for this document is the members of the working groups developing or making use of protocols. For the measures described in this part of IEC 62351 to take effect, they shall be accepted and referenced by the specifications for the protocols themselves.

The subsequent audience for this document is the developers of products that implement these protocols and the end user that want to specify requirements for its own environment.

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



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

### 1.2 Code components

The purchase of this IEC standard carries a copyright license for the purchaser to sell software containing Code Components from this standard to end users either directly or via distributors, subject to IEC software licensing conditions, which can be found at: www.iec.ch/CCv1.

The Code Components included in this IEC standard are also available as electronic machine readable file at: *www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN.1*_XSD.full.zip

In this document, code components are contained within Annexes A, B, C, D and E.

## 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 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD1:2018

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

IEC 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 8073:1997 | Rec. ITU-T X.224 (1995), *Information technology – open systems interconnection – Protocol for providing the connection-mode transport service*

ISO/IEC 8823-1:1994 | Rec. ITU-T X.226 (1994), *Information technology – open systems interconnection – connection-oriented presentation protocol: Protocol specification*

ISO/IEC 8824-1 | Rec. ITU-T X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1 | Rec. ITU-T X.690, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8825-4 | Rec. ITU-T X.693, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

AVA Documents
Document Sharing Hub



Full document details: BS EN IEC 62351-4:2018+A1:2020

ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*

〈A1〉 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks* 〈A1〉

Rec. ITU-T X.227 (1995), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification*

NOTE 1 The corresponding International Standard ISO/IEC 8650-1:1996 has been withdrawn.

Rec. ITU-T X.227 (1995)/Amd.1 (1996), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification – Amendment 1: Incorporation of extensibility markers*

NOTE 2 The corresponding International Standard amendment ISO/IEC 8650-1:1996/Amd.1:1997 has been withdrawn.

IETF RFC 1006:1987, *ISO Transport Service on top of the TCP, Version: 3*

IETF RFC 2104:1997, *HMAC: Keyed-Hashing for Message Authentication*

IETF RFC 3526:2003, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*

IETF RFC 5114:2008, *Additional Diffie-Hellman Groups for Use with IETF Standards*

IETF RFC 5246:2008, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information*

IETF RFC 5639:2010, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*

IETF RFC 5869:2010, *HMAC-based Extract-and-Expand Key Derivation Function*

IETF RFC 6120:2011, *Extensible Messaging and Presence Protocol (XMPP): Core*

IETF RFC 6122:2011, *Extensible Messaging and Presence Protocol (XMPP): Address Format*

## 3 Terms, definitions and abbreviated terms

### 3.1 General

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following 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



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

## 3.2 Terms and definitions

**3.2.1**
**a-security profile**
application security specification that provides peer-to-peer authentication as originally defined by IEC TS 62351-4:2007

**3.2.2**
**abstract syntax**
specification of application-protocol-data-units by using notation rules that are independent of the encoding technique used to represent them

[SOURCE: ISO/IEC 7498-1:1994 | Rec. ITU-T X.200 (1994), 7.1.1.2]

**3.2.3**
**alarm**
security event that might be caused by an adversary

**3.2.4**
**Application context**
set of rules shared in common by two application-entity in order to support an association (in an OSI operational environment)

**3.2.5**
**application entity**
active element embodying a set of capabilities which is pertinent to communication systems and which is defined for the application layer

**3.2.6**
**application profile**
application profile that represents the set of protocols and agreements in regards to the upper three layers of the OSI reference model

**3.2.7**
**application-protocol-control information**
information exchanged between application entities to co-ordinate their joint operation

**3.2.8**
**association**
cooperative relationship between application-entity invocations, which enables the communication of information and the coordination of their joint operation for an instance of communication

Note 1 to entry: This relationship may be formed by the transfer of application-protocol-control-information using an underlying service.

[SOURCE: Rec. ITU-T X.217 (1995), 3.5.1]

**3.2.9**
**association control service element**
application service element that provides the exclusive means for establishing and terminating application associations within an OSI environment

**3.2.10**
**bilateral agreement**
agreement between two control centres which includes the data elements to be accessed and the means to access them

[SOURCE: IEC 60870-6-503:2014, 3.3]



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

**3.2.11**
**bilateral table**
computer representation of the bilateral agreement

Note 1 to entry: The representation used is a local matter

[SOURCE: IEC 60870-6-503:2014, 3.4]

**3.2.12**
**CA certificate**
public-key certificate for one certification authority (CA) issued by another CA or by the same CA

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.14]

**3.2.13**
**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 | Rec. ITU-T X.509 (2019), 3.5.21]

**3.2.14**
**client**
application entity that initiate the establishment of an association with a server

Note 1 to entry: The term specifies the role of an entity for a particular association. The entity may have another role for another association.

Note 2 to entry: XMPP has a somewhat different client/server concept.

**3.2.15**
**compatibility mode**
operation mode where the partners in an association or in an association establishment communicate using those facilities specified by this part of IEC 62351 that corresponds to the facilities specified by IEC TS 62351-4:2007

**3.2.16**
**coordinated universal time**
UTC
time-scale maintained by BIPM (International Bureau of Weights and Measures or Bureau international des poids et mesures) that forms the basis of a coordinated dissemination of standard frequencies and time signals

Note 1 to entry: UTC and Greenwich Mean Time (GMT) are two alternative time standards that for most practical purposes determine the same time.

Note 2 to entry: Specified in Rec. ITU-R TF.460-6.

Note 3 to entry: ASN.1 has two built-in types for the representation of UTC, **`UTCTime`** and **`GeneralizedTime`**. **`UTCTime`** has a two-digit year representation, while **`GeneralizedTime`** has a four-digit year representation.

**3.2.17**
**data transfer phase**
phase from the completion of the establishment of an association to the initiation of the association termination

Note 1 to entry: In some specifications, this phase is termed a session. This term is avoided here, as it is used for other purposes within the OSI architecture and within TLS.



AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-4:2018+A1:2020

**3.2.18**
**E2E security**
security facilities at the application layer that ensures data origin authentication and integrity end-to-end with or without confidentiality (encryption) between two entities with zero or more intermediate entities

**3.2.19**
**end-entity public-key certificate**
public-key certificate issued to an entity, which then acts as an end entity within a public-key infrastructure

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.31]

**3.2.20**
**environment protocol data unit**
application protocol data unit (APDU) that is carrying protocol control information for the environment protocol in addition to carrying a security protocol data unit

**3.2.21**
**error**
security event that is caused by bad implementation behaviour resulting in disruption of communication

**3.2.22**
**internet protocol suite**
set of network communications protocols and a description framework used for the Internet and similar networks

Note 1 to entry: This is commonly also known as the TCP/IP suite or the TCP/IP model.

**3.2.23**
**native mode**
scenario where the partners in an association or an association establishment apply E2E security according to this part of IEC 62351 and possibly support TLS

**3.2.24**
**nonce**
number used once, either to protect against replay attacks or as initialization vector for cryptographic algorithms

**3.2.25**
**presentation data value**
unit of information specified in an abstract syntax, which is transferred by the underlying service in an OSI operational environment

**3.2.26**
**protected (application) protocol**
application protocol that is protected by E2E security

**3.2.27**
**protected protocol data unit**
application protocol data unit (APDU) defined by a protected application protocol

**3.2.28**
**protocol control information**
information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

**3.2.29**
**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 | Rec. ITU-T X.509.

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.58]

**3.2.30**
**salt**
random string used to add entropy to another, possibly random value.

Note 1 to entry: Salt may also be concatenated with a password before hashing to prevent collision and to protect against replay.

**3.2.31**
**secure protocol data unit**
application protocol data unit (APDU) carrying security protocol control information and, when relevant, carrying a protected protocol data unit

**3.2.32**
**server**
entity that accepts association request from clients

Note 1 to entry: The term specifies the role of an entity for a particular association. The entity may have another role for another association.

**3.2.33**
**transport profile**
profile that represents the protocols and agreements in regards to the lower four layers of the OSI reference model

**3.2.34**
**trust anchor**
an entity that is trusted by a relying party and used for validating public-key certificates

[SOURCE: ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019), 3.5.72]

**3.2.35**
**XML stanza**
a stanza is the basic unit of meaning in XMPP. A stanza is a first-level element (at depth=1 of the stream) whose element name is "message", "presence", or "iq" and whose qualifying an XML namespace is ’jabber:client’ or ’jabber:server’

[SOURCE: IETF RFC 6120:2011, 4.1]

### 3.3 Abbreviated terms

For the purposes of this document, the abbreviated terms given in IEC TS 62351-2 and the following apply.

| | |
|---|---|
| ACSE | Association Control Service Element |
| AE | Authenticated Encryption |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| BER | Basic Encoding Rules |



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

| | |
|---|---|
| CA | Certification Authority |
| CBC | Cipher Block Chaining |
| CRL | Certificate Revocation List |
| DER | Distinguished Encoding Rules |
| DHE | Ephemeral Diffie-Hellman |
| E2E | End-to-End |
| ECDHE | Elliptic Curve Ephemeral Diffie-Hellman |
| EnvPDU | Environment Protocol Data Unit |
| GCM | Galois/Counter Mode |
| GMAC | Galois Message Authentication Code |
| HKDF | HMAC-based Extract-and-Expand Key Derivation Function |
| HMAC | Keyed-hash Message Authentication Code |
| ICCP | Inter-Control Centre Communications Protocol |
| ICV | Integrity Check Value |
| IPsec | Internet Protocol security |
| JID | Jabber Identifier |
| MAC | Message Authentication Code |
| MMS | Manufacturing Message Specification |
| OCSP | Online Certificate Status Protocol |
| PCI | Protocol Control Information |
| PDU | Protocol Data Unit |
| PDV | Presentation Data Value |
| PPDU | Presentation Protocol Data Unit |
| PrPDU | Protected Protocol Data Unit |
| SecPDU | Security Protocol Data Unit |
| SPDU | Session Protocol Data Unit |
| TASE.2 | Telecontrol Application Service Element 2 |
| TPDU | Transport Protocol Data Unit |
| UTC | Coordinated Universal Time |
| VPN | Virtual Private Network |
| XER | XML Encoding Rules |
| XML | eXtensible Markup Language |
| XMPP | eXtensible Messaging and Presence Protocol |
| XSD | XML Schema Definition |



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

# 4 Security issues addressed by this part of IEC 62351

## 4.1 Communications reference models

Figure 1 illustrates the OSI reference model and how an OSI protocol stack and an Internet protocol suite relate to that model.

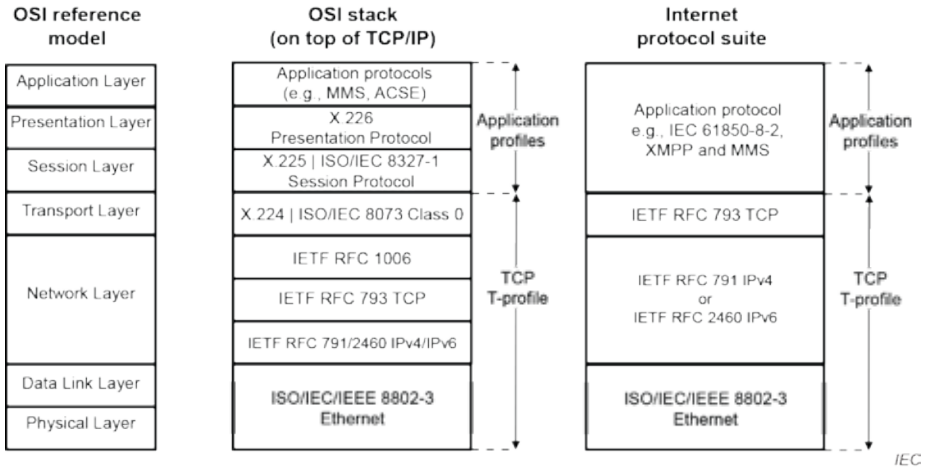


**Figure 1 – Application and transport profiles (informative)**

In relation to this document and in most other cases, the OSI stack is a hybrid stack allowing application based on an OSI stack, such as Manufacturing Message Specification (MMS), to communicate over a TCP/IP based network, such as the public Internet. The top four layers are OSI protocols, while the OSI network service is provided by IETF RFC 1006 on top of a TCP/IP stack.

In the Internet protocol suite, the three top OSI layers are collapsed into one application layer.

## 4.2 Security for application and transport profiles

The communications aspect, as relevant for this document and shown in Table 1, is discussed in terms of:

a) Transport profiles: A transport Profile (T-profile) defines the set of protocols and requirements for layers 1 to 4 of the OSI Reference Model.

b) Application profiles: An application profile (A-profile) defines the sets of protocols and requirements for layers 5 to 7 of the OSI Reference Model.

This is also illustrated in Figure 1.

There are two T-security specifications and two application security specifications identified by this part of IEC 62351.

In the terms of security, the T-security, if present, is typically provided by transport layer security (TLS) as defined by IETF RFC 5246.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

**Table 1 – Relationship between security and security measure combinations**

| **Application Security** | A-security profile | None | A-security profile | E2E security without encryption | E2E security without encryption | E2E security with encryption | E2E security with encryption |
|---|---|---|---|---|---|---|---|
| **Transport Security** | none | TLS | TLS | none | TLS | none | TLS |
| **Note** | Note 1 | Note 2 | | Note 3 | | Note 4 | |
| For the application of the T-security, TLS is expected to be used as specified in 6.3 for the OSI operational environment. For other environments, TLS usage is outside the scope of this document and specified by the referencing standard.<br><br>Note 1: Using the A-security profile alone without TLS results in a non-secure system.<br><br>Note 2: Using TLS with or without the A-security profile gives a reasonable security assuming that all other security measures are observed, including use of secure TLS cipher suits and that the communication is peer-to-peer without intermediate entities. In addition to the authentication provided by TLS, the use of the A-security profile allows for authentication at the application layer of application entities.<br><br>Note 3: Using E2E security without encryption with or without TLS provides for mutual authentication and end-to-end integrity protection and thus reasonable security providing that confidentiality is not required and that other security measures are observed. Use of TLS fulfils confidentiality (encryption) an integrity protection on transport layer hops should the E2E security be compromised.<br><br>Note 4: As for note 3 with addition of end-to-end encryption (confidentiality). | | | | | | | |

NOTE If in an ICCP environment confidentiality is needed and no encryption, as specified by this part of IEC 62351-4, is being utilized, it is suggested to utilize some other form of encryption technology such as a VPN.

### 4.3 Compatibility and native modes

This document specifies two mutually exclusive modes of operation. i.e., communication is done exclusively in either of the two modes:

a) The compatibility mode is a mode of operation that is compatible with IEC TS 62351-4:2007. The set of cipher suits for TLS used in this mode is specified in 6.3.4.2 and the application security specification is given in Clause 11.

   The mode of operation is only relevant for MMS in an OSI operational environment by reference to ISO 9506-2:2003 and Rec ITU-T X.227:1995. This mode of operation is not recommended for new implementations.

b) The native mode of operation represents the major addition to this document. It allows for extended support for TLS as specified in 6.3.4.3 and it allows for end-to-end security between two application entities with zero or more intermediate application entities as specified in Clauses 12 to 16.

### 4.4 Security threats countered

#### 4.4.1 General

See IEC TS 62351-1 for a discussion on security threats and attack methods.

The listed security threats are mitigated through the appropriate implementation of the specification/recommendations found within this document.

The security threats countered depend on whether compatibility mode or native mode of operation is used.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

#### 4.4.2 Threats countered in compatibility mode

If IEC 62351-3:2018 is not employed for data to be transmitted, but the A-security profile applies, then the specific threat countered includes:

– Masquerade during association establishment.

If IEC 62351-3:2018 is employed, then, in addition to above, the specific threats countered include:

– Unauthorized modification (tampering) of information by use of digital signatures and integrity check values (ICVs), the latter is also referred to as message authentication codes (MACs).
– Theft or misuse of information by use of confidentiality (encryption).

#### 4.4.3 Threats countered in native mode

If TLS is employed, then on the individual hops the specific threats countered include:

– Masquerade during connection establishment.
– Unauthorized modification (tampering) of information by use of digital signatures and integrity check values (ICVs).
– Theft or misuse of information by use of confidentiality (encryption).

For E2E security without encryption, the specific threat countered in the end-to-end communications includes:

– Masquerade during association establishment end-to-end.
– Unauthorized modification (tampering) both for the handshake phase and for the data transfer phase by use of digital signatures and integrity check values (ICVs) end-to-end.
– Replay countered through the use of time, association ID and sequence numbers.

For E2E security with encryption, the additional specific threat countered includes:

– Theft or misuse of information by use of confidentiality (encryption) end-to-end.

### 4.5 Attack methods countered

#### 4.5.1 General

The attack methods countered depend on whether compatibility mode or native mode is used.

#### 4.5.2 Attacks countered in compatibility mode

The following list is exclusive of the attack methods countered through the deployment of IEC 62351-3:2018, as outlined within this document:

– Man-in-the-middle: This threat is countered through the use of authentication during TLS handshake by use of digital signature and during data transfer by use of ICV.
– Tamper detection/message integrity: This attack is countered in the same way as the man-in-the-middle attack.
– Masquerading: This attack is countered in the same way as the man-in-the-middle attack.

#### 4.5.3 Attacks countered in native mode

If TLS is employed, then on the individual hops the specific attacks countered include:

– Man-in-the-middle: This threat is countered through the use of authentication during TLS handshake by use of digital signature and during data transfer by use of ICV.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

– Tamper detection/message integrity: This attack is countered in the same way as the man-in-the-middle attack.
– Masquerading: This attack is countered in the same way as the man-in-the-middle attack.

For E2E security without encryption, the specific attacks countered in the end-to-end communications includes:

– Man-in-the-middle: 〚A1〛This threat is countered through the use of authentication during end-to-end association establishment by use of digital signature and during data transfer by use of ICV.〚A1〛
– Tamper detection/message integrity: This attack is countered in the same way as the man-in-the-middle attack.
– Masquerading: This attack is countered in the same way as the man-in-the-middle attack.
– Replay: This attack is countered through the use time and sequence numbers.

For E2E security with encryption, the additional specific attack countered includes:

– Theft or misuse of information by use of confidentiality (encryption) end-to-end.

### 4.6 Logging

It is important that care be taken to log security-related violations in a separate log whose contents are inherently secure from manipulation (e.g., modification of information or deletion of information). Implementers should strive to archive enough information so that security audit and prosecution is facilitated. The actual implementation of this recommendation is a local matter.

Relevant communications and definitions pertaining to monitoring and security logging are addressed in two separate parts of IEC 62351: IEC 62351-7 targets monitoring in the context of network management, while IEC 62351-14 addresses security logging.

## 5 Specific requirements

### 5.1 Specific requirements for ICCP/IEC 60870-6-x communication stack

This Clause is relevant and normative when this part of IEC 62351 is used in connection with ICCP also referred to as Telecontrol Application Service Element 2 (TASE.2), as defined in IEC 60870-6-503:2014 [2], IEC 60870-6-702:2014 [3] and IEC 60870-6-802:2014 [4].

The implementation of MMS for ICCP shall provide some mechanism for configuring and making use of the security capabilities. This is provided as bilateral agreements as specified in IEC 60870-6-503:2014.

In general, the following needs to be provided:

– A mechanism for configuration of public-key certificate information and the binding of that information to access authentication (e.g., the bilateral tables).
– A mechanism for configuration of the acceptable incoming transport profile for the implementation's access control mechanism. It is suggested that the following choices be provided:
  - DON'T_CARE: An MMS association may be established with or without the use of T-security.
  - NON_SECURE: would indicate that T-security shall not be used in order to allow establishment of an MMS association.
  - SECURE: would indicate that T-security shall be used in order to allow establishment of an MMS association.



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

– A mechanism for configuration of the application security to use in order to initiate an MMS association. It is suggested that the following choices be provided:
  - NON_SECURE: would indicate that an application security shall not be used in order to allow establishment of an MMS association.
  - SECURE: would indicate that the A-security profile as specified in Clause 11 (or IEC TS 62351-4:2007) shall be used in order to allow establishment of an MMS association.
  - END-TO-END SECURE: would indicate that E2E security shall be used in order to allow establishment of an MMS association.
– A mechanism to convey/verify the association parameters. These parameters should include address information, profile used indication (e.g., end-to-end secure, secure, or non-secure) and handshake authentication parameters.

  This information shall be used, in conjunction with the configured MMS expected association values, to determine if an MMS association should be established. How the entity determines the actual acceptance is a local issue.

When having to restart a single association due to configuration changes, it is desirable that this does not require other associations to be restarted. However, some referencing specifications require a complete restart of all associations.

### 5.2 Specific requirements for IEC 61850

When a referencing standard of the IEC 61850 series wants to run in compatibility mode, it shall specify the application context **`basic-AC`** (see 11.1.4.2) in the association request. If it wants to run in native mode, it shall specify the application context **`e2eMmsAC`** (see 15.2.2).

## 6 Transport Security

### 6.1 General

The T-security does not specify security recommendations for TCP, IP, or Ethernet. Rather the specifications for T-security define how to apply Transport Layer Security (TLS) properly to secure traffic above the transport layer. This specification relates in part to the TLS profile defined in IEC 62351-3:2018.

### 6.2 Application of transport layer security (TLS)

#### 6.2.1 General

A general profile of TLS is specified in IEC 62351-3:2018 which leaves many parameters open. Subclauses, 6.2.2 through 6.2.9, describe and define the required values and settings of these parameters for compliance with this document. The types of parameters specified include:

a) The mandatory TLS cipher suites to be supported.
b) The recommended specification in regards to resumption of session parameters from a previous connection based upon session run-time.
c) The recommended specification in regards to the renegotiation of session parameters based upon session run-time.
d) The recommended default certificate revocation list (CRL) evaluation period if CRLs are used for revocation checking.
e) In case of using OCSP for certificate revocation checks, the handling of failures to access the OCSP responder.
f) The handling of public-key certificate validation actions.
g) The conformance requirements to this part of IEC 62351. The conformance statement is provided in Clause 17.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

Besides the parameters already required by IEC 62351-3:2018 and specified in this clause, further specification of selected parameters is required as defined in Clause 6.3 for OSI operational environment and Clause 6.4 for the XMPP operational environment.

### 6.2.2 The TLS cipher suite concept

A cipher suite in TLS is a set of cryptographic algorithms for the combination of peer authentication, encryption, message authentication code (MAC), and key exchange algorithms. A cipher suite is identified by a specific cipher suite value used in the ClientHello and the ServerHello messages. These values are registered by IANA in the TLS Cipher Suite Registry.

### 6.2.3 TLS session resumption

An implementation that claims conformance to this specification shall support session resumption at least every two hours.

NOTE This requirement is not applicable for support of compatibility mode.

### 6.2.4 TLS session renegotiation

An implementation that claims conformance with this document shall support session renegotiation with at least half of the CRL update period (see also 6.2.7).The lower bound for the session renegotiation shall be 10 minutes.

NOTE This requirement protects client and server performance by preventing too many full TLS handshakes and associated public-key certificate validations.

### 6.2.5 Supported number of trust anchors

Implementations compliant to this specification shall support at least two different trust anchors. That requirement aligns with the certificate management described in IEC 62351-9 describing vendor and operator distributed public-key certificates.

### 6.2.6 Public-key certificate size

A1 An implementation that claims conformance to this document shall support a public-key certificate size of minimum and maximum 8192 octets. It is a local issue if larger public-key certificates are supported.

In order to achieve interoperability of public-key certificates, it is necessary to set a maximum allowed size for the public-key certificates exchanged by ACSE. This size shall be limited to a maximum encoding size of 8192 octets. A1

An implementation that receives a public-key certificate larger than the size that it can support shall terminate the connection and shall raise a security event ("warning: session termination due to unsupported public-key certificate size").

### 6.2.7 Evaluation period for revocation state of public-key certificates

An implementation that claims conformance to this part of IEC 62351 shall support a CRL refresh at minimum every 24 hours. The default evaluation period for revoked public-key certificates shall be 24 hours. This evaluation period shall be configurable.

An implementation supporting OCSP for revocation check information shall cache the OSCP response no longer than 24 hours.

An inability to access the CRL provider or the OCSP responder or a locally cached CRL or OCSP response shall raise a security event ("warning: certificate revocation information unavailable").



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

In line with to IEC 62351-3:2018, the inability to retrieve the revocation information shall not cause the session to be terminated.

### 6.2.8 Public-key certificate validation

An implementation that claims conformance to this specification shall, subject to local policy, be able to terminate a connection establishment or connection renegotiation, where one of the public-key certificates used by either the client or the server is revoked or has been expired.

The refusal of a connection establishment or the termination of a connection during session renegotiation due to a revoked or expired public-key certificate should raise a security event ("incident: revoked public-key certificate"). If the public-key certificate had expired, a security event ("warning: expired public-key certificate") shall be raised.

### 6.2.9 Security events handling

Security event and monitoring information should be made available to the embedding infrastructure through the application of IEC 62351-7:2017 and/or IEC 62351-14. IEC 62351-7:2017 defines the handling of security monitoring information, while IEC 62351-14 specifies the handling of security warning and security incident messages.

## 6.3 T-security in an OSI operational environment

### 6.3.1 General

TLS as specified for T-security shall be used as specified by IEC 62351-3:2018 with the specified parameter set in 6.2. Subclauses 6.3.2 through 6.3.4 further specify the communication ports and cipher suites to be utilized.

### 6.3.2 TCP ports

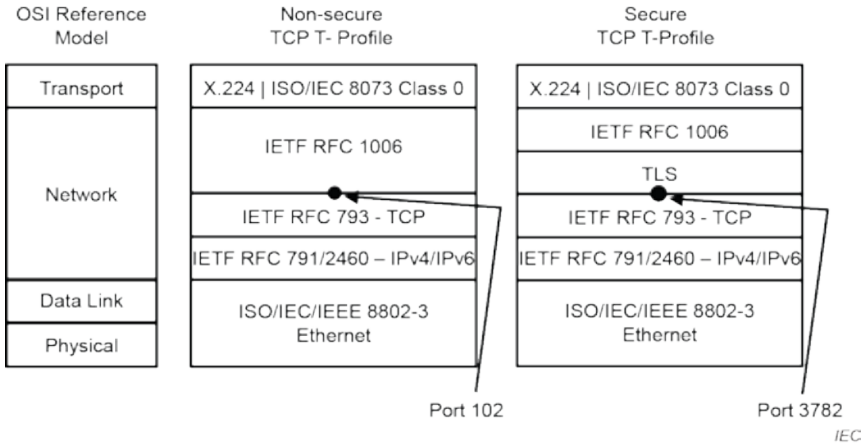


**Figure 2 – T-profiles without and with TLS protection**

Figure 2 shows the two relevant TCP T-Profiles. One is the standard IETF RFC 1006 T-Profile that provides no transport security. The other one shows the addition of TLS to provide transport security as specified within this document.

When there is no transport security, TCP port 102 shall be used as specified by IETF RFC 1006.

Implementations claiming conformance to this part of IEC 62351-4 shall use TCP port 3782 to indicate the use of the transport security. This port is registered by IANA as a secure ISO TP0 port.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

IETF RFC 1006 only supports the use of transport class 0 of ISO/IEC 8073 | Rec. ITU-T X.224.

### 6.3.3 Disabling of TLS

Implementations shall permit TLS to be disabled. When disabled, the TCP port 102 shall be used.

TLS may be disabled depending on the underlying security, which may be provided through a VPN (used in this context to describe a security protocol below TLS, which may be IPsec or another) or depending on the utilized application security profile.

### 6.3.4 TLS cipher suites support

#### 6.3.4.1 General

6.3.4.2 defines TLS cipher suites to be supported in compatibility mode, and 6.3.4.3 defines TLS cipher suites to be supported in native mode. Referencing specifications may add additional mandatory cipher suites.

A1 TLS prioritizes the proposed cipher suites in the TLS handshake according to the order in the proposed cipher suite list in the ClientHello message. To accommodate a security policy it is strongly recommended to have the order of proposed cipher suites according to the local security policy. Cipher suites marked as mandatory shall be stated in the proposal list of the ClientHello message. A1

#### 6.3.4.2 Mandatory and recommended cipher suites for compatibility mode

A1 All implementations that claim conformance to IEC TS 62351-4:2007 shall support TLS_DH_DSS_WITH_AES_256_CBC _SHA at a minimum. A1

It is recommended that the TLS cipher suites listed in Table 2 (from IEC TS 62351-4:2007) be considered. Due to advances in cryptography, certain cipher suites are considered insecure. These are marked in the original table from IEC TS 62351-4:2007.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

**Table 2 – Commented recommended cipher suites from IEC TS 62351-4:2007**

| Key exchange | | Encryption | Hash | IANA Value | Source | Support |
|---|---|---|---|---|---|---|
| Algorithm | Signature | | | | | |
| TLS_RSA_ | | WITH_RC4_128_ | SHA | 0x00,0x05 | RFC 2246 (TLS 1.0) | Disallowed (RC 4 considered weak) |
| TLS_RSA_ | | WITH_3DES_ede_CBC_ | SHA | 0x00,0x0A | RFC 2246 (TLS 1.0) | o |
| TLS_DH_ | DSS_ | WITH_3DES_ede_CBC_ | SHA | 0x00,0x0D | RFC 2246 (TLS 1.0) | o |
| TLS_DH_ | RSA_ | WITH_3DES_ede_CBC_ | SHA | 0x00,0x10 | RFC 2246 (TLS 1.0) | o |
| TLS_DHE_ | DSS_ | WITH_3DES_ede_CBC_ | SHA | 0x00,0x13 | RFC 2246 (TLS 1.0) | o |
| TLS_DHE_ | RSA_ | WITH_3DES_ede_CBC_ | SHA | 0x00,0x16 | RFC 2246 (TLS 1.0) | o |
| TLS_DH_ | DSS_ | WITH_AES_128_CBC_ | SHA | 0x00,0x30 | RFC 4346 (TLS 1.1) | o |
| TLS_DH_ | DSS_ | WITH_AES_256_CBC_ | SHA | 0x00,0x36 | RFC 4346 (TLS 1.1) | m |
| TLS_DH_ | | WITH_AES_128_CBC | SHA | 0x00, 0x34 | RFC 4346 (TLS 1.1) | Disallowed (anonymous) |
| TLS_DH_ | | WITH_AES_256_CBC | SHA | 0x00, 0x3A | RFC 4346 (TLS 1.1) | Disallowed (anonymous) |

NOTE The negotiation mechanism in TLS selects the actual cipher suite used for a particular connection based upon the configured allowed/present cipher suites.

#### 6.3.4.3 Mandatory and recommended cipher suites for native mode

All implementations that claim conformance to the native mode shall support the mandatory cipher suites listed in Table 3.

It is recommended that the optional TLS cipher suites listed in Table 3 be considered for use. They originate from different IETF RFCs as noted in Table 3.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

**Table 3 – Cipher suites combinations in the context of this document**

| Key exchange | | Encryption | Hash | IANA Value | Source | Support |
|---|---|---|---|---|---|---|
| Algorithm | Signature | | | | | |
| TLS_RSA | | WITH_AES_128_CBC_ | SHA256 | 0x00,0x3C | RFC 5246 | m |
| TLS_DH_ | RSA_ | WITH_AES_128_CBC_ | SHA256 | 0x00,0x31 | RFC 5246 | o |
| TLS_DH_ | RSA_ | WITH_AES_128_GCM_ | SHA256 | 0x00,0xA0 | RFC 5288 [20] | m |
| TLS_DHE_ | RSA_ | WITH_AES_128_GCM_ | SHA256 | 0xC0,0x9E | RFC 5288 [20] | m |
| TLS_DH_ | RSA_ | WITH_AES_256_GCM_ | SHA384 | 0x00,0xA1 | RFC 5288 [20] | o |
| TLS_ECDHE_ | RSA_ | WITH_AES_128_GCM_ | SHA256 | 0xC0,0x2F | RFC 5289 [7] | o |
| TLS_ECDHE_ | RSA_ | WITH_AES_256_GCM_ | SHA384 | 0xC0,0x30 | RFC 5289 [7] | o |
| TLS_ECDHE_ | ECDSA_ | WITH_AES_128_GCM_ | SHA256 | 0xC0,0x23 | RFC 5289 [7] | m |
| TLS_ECDHE_ | ECDSA_ | WITH_AES_256_GCM_ | SHA384 | 0xC0,0x24 | RFC 5289 [7] | o |

### 6.4 T-security in an XMPP operational environment

TLS for T-security in an XMPP environment shall be used as specified by Clause 5 of IETF RFC 6120:2011. Subclauses 13.7.2 to 13.7.4 of this RFC provide the specification for public-key certificate handling and require the support of the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. As this cipher suite is considered less secure due to the application of SHA-1, this part of IEC 62351 instead strongly recommends the support of the TLS_RSA_WITH_AES_128_CBC_SHA256 cipher suite to be more future proof. Additionally, the specified parameter set in Clause 6.2 is recommended to be considered.

IETF RFC 7590 provides additional requirements on the XMPP use of TLS. This IETF RFC requires that the recommendations given in IETF RFC 7525 shall be followed.

Referencing standards of this document shall determine the necessary T-profile parameters.

## 7 Application layer security overview (informative)

### 7.1 General

While the T-security provides authentication, integrity and confidentiality at the transport layer, application security provides security at the application layer.

This part of IEC 62351 specifies two classes of application security capabilities:

a) A peer-to-peer security specification, called the A-security profile, which is equivalent to the A-profile specified by IEC TS 62351-4:2007, only provides security for MMS based application protocols and only supports an OSI protocol stack. It is provided here, as communities such as ICCP community and as IEC 61850-8-1 implementations are using this security specification. In general, it is strongly recommended to migrate to stronger security. This security specification only provides peer authentication at the application layer during association establishment, with no cryptographic binding for the subsequent data exchange messages (data transfer phase). It does not provide for end-to-end authentication with intermediate entities and it does not provide for integrity and confidentiality. This profile should only be used together with T-security.

   The specification for the A-security profile is given in Clause 11.

b) End-to-end application security, named E2E security, which provide end-to-end security at the application layer with zero or more intermediate entities (while T-security only provides security on the individual hops).

   E2E security can be applied in different operational environment and it can protect different protocols.



AVA Documents Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

The E2E security provides end-to-end data origin authentication and message integrity during association establishment and for the subsequent data transfer phase bound to the initial authentication. E2E security can be used without or with encryption.

Although the security information is exchanged end-to-end, an intermediate entity is somewhat involved, like when it is not possible to perform the routing.

The specification for the E2E security is given in the following clauses:

- A1 Clause 12 defines the overall model or architecture for E2E security, including how E2E security relates to an operational environment and a protected protocol. A1
- Clause 13 specifies the protocol for the E2E security independent of operational environment and the protected protocol.
- Clause 14 specifies procedures for the E2E security error handling.
- Clause 15 specifies the requirements for an OSI operational environment, including specific error handling.
- Clause 16 specifies the requirements for an XMPP operational environment, including specific error handling.

## 7.2 Description techniques

### 7.2.1 General

The Abstract Syntax Notation ONE (ASN.1), as specified in ISO/IEC 8824-1 | Rec. ITU-T X.680, is used for specifying the E2E security protocol. Use of ASN.1 is further discussed in 7.2.2.

The abstract syntax for the E2E security protocol is also expressed in W3C XML Schema Definition (W3C XSD) as specified in W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures [8] and in W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes [9]. Use of W3C XSD is further discussed in 7.2.3.

### 7.2.2 ASN.1 as an XML schema definition

The formal ASN.1 specification for E2E security is given in Annex B.

There are different encoding rules for an ASN.1 abstract syntax:

a) In an OSI operational environment, including the A-security profile, this part of IEC 62351 requires the support of basic encoding rules (BER) as specified by ISO/IEC 8825-1 | Rec. ITU-T X.690.

b) In an XMPP environment, the encoding may be based on the ASN.1 specification using the XML encoding rules (XER) or more precise, the A1 EXTENDED-XER A1 as specified by ISO/IEC 8825-4 | Rec. ITU-T X.693.

c) According to ISO/IEC 9594-8 | Rec. ITU-T X.509, public-key certificates and attribute certificates shall be encoded using distinguished encoding rules (DER). DER is BER with some restrictions that remove all encoding options. An implementation shall check that public-key and attribute certificates are DER encoded. A1 DER is also specified by ISO/IEC 8825-1 | Rec. ITU-T X.690. A1

### 7.2.3 W3C XML Schema Definition (W3C XSD)

W3C XSD is an alternative abstract syntax that may be used for XML encoding of PDUs.

If XML encoding is required, either W3C XSD or ASN.1 EXTENDED-XER shall be supported.

As specified in 7.2.2 c), public-key and attribute certificates shall be encoded in ASN.1 DER. An implementation using XSD shall be able to validate a public-key or attribute certificate encoded in DER. An implementation using W3C XSD shall also be aware that all PKI related communications (CRL retrieval, OCSP access, etc.) require ASN.1 BER encoding.



AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

The W3C XSD for the E2E security is given in Annex C.

### 7.2.4 XML namespace

When XML encoding is required, the E2E security and the virtual-API (see A1 16.5 A1) share a common XML namespace identified as **http://www.iec.ch/62351/2018/E2E_4**.

## 8 Use of cryptographic algorithms

### 8.1 General

This document makes extensive use of cryptographic algorithms for providing the required security. This Clause introduces relevant cryptographic algorithms to be used by either the A-security profile or E2E security. Clause 11 specifies the cryptographic algorithm to be used for the A-security profile, while Clause 13 specifies the cryptographic algorithms to be used for E2E security.

ISO/IEC 9594-8 | Rec. ITU-T X.509 defines different ASN.1 constructs for formal specifications of cryptographic algorithms. These definitions are copied into 8.2 for easy reference. 8.3 to 8.8 list cryptographic algorithms as defined by other specifications, such as IETF RFCs. These algorithms are considered relevant for this document.

### 8.2 Basic cryptographic definitions

```
ALGORITHM::= CLASS {
  &Type           OPTIONAL,
  &id             OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
  [PARMS          &Type]
  IDENTIFIED BY   &id }
```

The **ALGORITHM** ASN.1 information object class is used for the formal specifications of cryptographic algorithms.

```
AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms}::= SEQUENCE {
  algorithm   ALGORITHM.&id({SupportedAlgorithms}),
  parameters  ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }
```

The **AlgorithmIdentifier** parameterized data type gives the general syntax for a cryptographic algorithm as defined using the **ALGORITHM** ASN.1 information object class.

The cryptographic algorithms are under continuous development. This part of IEC 62351 is open for new and more secure algorithms. The following algorithm specifications are those that are considered safe to be used for an extended period. Referencing specifications and/or implementers' agreements may add to the list of cryptographic algorithms to be used for specific environments.

ASN.1 has a concept of ASN.1 object sets that allows a specification to specify a supported set of cryptographic algorithms for a specific purpose as illustrated by the example below:

```
AlgorithmSet ALGORITHM::= {
  algorithm-ID1 |
  algorithm-ID2 |
   - - -
  algorithm-IDn,
  ... }
```

A1 A defined set represents a set of cryptographic algorithms relevant for a particular situation.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020

The extension mark ( ... ) will cause an ASN.1 tool to accept any cryptographic object, whether it identifies a cryptographic algorithm for the specific purpose or not. A referencing specification or an implementers' agreement may remove the extension mark and/or add additional algorithms. 〈A1〉

### 8.3 Public-key algorithms

Two public-key algorithms are introduced here:

```
rsaEncryptionAlgorithm ALGORITHM::= {
  PARMS         NULL
  IDENTIFIED BY rsaEncryption }

rsaEncryption      OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

IETF RFC 4055 gives the formal specification for the `rsaEncryptionAlgorithm` public-key algorithms.

```
ecPublicKey ALGORITHM::= {
  PARMS         OBJECT IDENTIFIER
  IDENTIFIED BY id-ecPublicKey }

id-ecPublicKey     OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840)
  ansi-x9-62(10045) keyType(2) 1 }       -- IETF RFC 5480
```

IETF RFC 5480 gives the formal specification for the `ecPublicKey` public-key algorithm.

The `ecPublicKey` public-key algorithm requires an identification of an elliptic curve as the parameter. A particular elliptic curve is identified by an object identifier. The following elliptic curves are relevant for this part of IEC 62351.

```
secp256r1          OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840)
  ansi-x9-62(10045) curves(3) prime(1) 7 }
```

IETF RFC 5480 gives the formal specification for the `secp256r1` elliptic curve.

```
brainpoolP256r1    OBJECT IDENTIFIER::= { iso(1) identified-organization(3)
  teletrust(36) algorithm(3) signature-algorithm(3) ecSign(2) 8 ellipticCurve(1)
  versionOne(1) 7 }
```

IETF RFC 5639 gives the formal specification for the `brainpoolP256r1` elliptic curve.

### 8.4 Hash algorithms

A single hash algorithm is introduced here:

```
sha256 ALGORITHM::= { -- IETF RFC 5754
  IDENTIFIED BY id-sha256 }

id-sha256 OBJEC IDENTIFIER::= { joint-iso-itu-t(2) country(16) us(840)
      organization(1) gov(101) csor(3) nistAlgorithm(4) hashalgs(2) 1 }
```

〈A1〉 IETF RFC 5754 gives the formal specification for the `sha256` hash algorithm. 〈A1〉

### 8.5 Signature algorithms

A signature algorithm is a combination of a hash algorithm and a public-key algorithm to be applied when generating and 〈A1〉 verifying 〈A1〉 digital signatures.

The following signature algorithms are relevant for this document.



Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-4:2018+A1:2020