

SS IEC 62541-6:2022
IEC 62541-6:2020, IDT
(ICS 25.040.40; 35.100.05)

SINGAPORE STANDARD
OPC unified architecture
– Part 6 : Mappings

SS IEC 62541-6:2022

IEC 62541-6:2020, IDT

(ICS 25.040.40; 35.100.05)

SINGAPORE STANDARD

OPC unified architecture

– Part 6 : Mappings

Published by Enterprise Singapore

**Enterprise
Singapore**



**THIS PUBLICATION IS COPYRIGHT
PROTECTED**

Copyright © 2022 Enterprise Singapore

Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from Enterprise Singapore, representing the IEC National Committee of Singapore, or the IEC. If you have any questions about the copyrights of Enterprise Singapore or the IEC or have an enquiry about obtaining additional rights to this publication, please contact Enterprise Singapore at: standards@enterprisesg.gov.sg for further information.

ISBN 978-981-5073-80-5

National Foreword

This Singapore Standard was prepared by the Working Group on Open Platform Communications unified architecture set up by the Technical Committee on Smart Manufacturing under the purview of the Manufacturing Standards Committee.

This standard is a revision of SS IEC 62541-6:2019 and is an identical adoption of IEC 62541-6:2020, “OPC unified architecture – Part 6 : Mappings”, published by the International Electrotechnical Commission”.

NOTE – Where appropriate, the words “International Standard” are read as “Singapore Standard”.

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

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “mature standards”. Mature standards will not be subject to further review, unless there are requests to review such standards.*
2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
3. *Compliance with a SS or TR does not exempt users from any legal obligations.*



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**OPC unified architecture –
Part 6: Mappings**

**Architecture unifiée OPC –
Partie 6: Mappings**





THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 IEC, Geneva, Switzerland

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

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

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

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

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

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC - webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**OPC unified architecture –
Part 6: Mappings**

**Architecture unifiée OPC –
Partie 6: Mappings**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-8596-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD	8
1 Scope	11
2 Normative references	11
3 Terms, definitions, abbreviated terms and symbols.....	13
3.1 Terms and definitions.....	13
3.2 Abbreviated terms and symbols	14
4 Overview	14
5 Data encoding	16
5.1 General.....	16
5.1.1 Overview	16
5.1.2 Built-in Types	16
5.1.3 Guid	17
5.1.4 ByteString.....	17
5.1.5 ExtensionObject	17
5.1.6 Variant.....	18
5.1.7 Decimal	18
5.2 OPC UA Binary	19
5.2.1 General	19
5.2.2 Built-in Types	19
5.2.3 Decimal	30
5.2.4 Enumerations	30
5.2.5 Arrays.....	30
5.2.6 Structures.....	31
5.2.7 Structures with optional fields	33
5.2.8 Unions	35
5.2.9 Messages	36
5.3 OPC UA XML.....	37
5.3.1 Built-in Types	37
5.3.2 Decimal	43
5.3.3 Enumerations	43
5.3.4 Arrays.....	44
5.3.5 Structures.....	44
5.3.6 Structures with optional fields	45
5.3.7 Unions	45
5.3.8 Messages	46
5.4 OPC UA JSON.....	46
5.4.1 General	46
5.4.2 Built-in Types	46
5.4.3 Decimal	52
5.4.4 Enumerations	52
5.4.5 Arrays.....	52
5.4.6 Structures.....	53
5.4.7 Structures with optional fields	53
5.4.8 Unions	54
5.4.9 Messages	54
6 Message SecurityProtocols	55

6.1	Security handshake	55
6.2	Certificates	56
6.2.1	General	56
6.2.2	Application Instance Certificate.....	57
6.2.3	Certificate Chains	58
6.3	Time synchronization	58
6.4	UTC and International Atomic Time (TAI).....	58
6.5	Issued User Identity Tokens.....	58
6.5.1	Kerberos.....	58
6.5.2	JSON Web Token (JWT).....	59
6.5.3	OAuth2	60
6.6	WS Secure Conversation	62
6.7	OPC UA Secure Conversation	62
6.7.1	Overview	62
6.7.2	MessageChunk structure	62
6.7.3	MessageChunks and error handling.....	67
6.7.4	Establishing a SecureChannel	67
6.7.5	Deriving keys.....	69
6.7.6	Verifying Message security	70
7	TransportProtocols	71
7.1	OPC UA Connection Protocol.....	71
7.1.1	Overview	71
7.1.2	Message structure	72
7.1.3	Establishing a connection	75
7.1.4	Closing a connection	77
7.1.5	Error handling.....	77
7.2	OPC UA TCP	79
7.3	SOAP/HTTP.....	79
7.4	OPC UA HTTPS.....	79
7.4.1	Overview	79
7.4.2	Session-less Services.....	81
7.4.3	XML Encoding	81
7.4.4	OPC UA Binary Encoding	82
7.4.5	JSON Encoding	82
7.5	WebSockets.....	83
7.5.1	Overview	83
7.5.2	Protocol Mapping.....	84
7.5.3	Security	84
7.6	Well known addresses	85
8	Normative Contracts	86
8.1	OPC Binary Schema	86
8.2	XML Schema and WSDL	86
8.3	Information Model Schema.....	86
8.4	Formal definition of UA Information Model.....	86
8.5	Constants	86
8.6	DataType encoding	86
8.7	Security configuration	86
Annex A (normative)	Constants.....	87
A.1	Attribute Ids	87

A.2	Status Codes	87
A.3	Numeric Node Ids	88
Annex B (normative)	OPC UA Nodeset	89
Annex C (normative)	Type declarations for the OPC UA native Mapping	90
Annex D (normative)	WSDL for the XML Mapping	91
D.1	XML Schema	91
D.2	WSDL Port Types	91
D.3	WSDL Bindings	91
Annex E (normative)	Security settings management	92
E.1	Overview	92
E.2	SecuredApplication	93
E.3	CertificateIdentifier	96
E.4	CertificateStoreIdentifier	98
E.5	CertificateList	99
E.6	CertificateValidationOptions	99
Annex F (normative)	Information Model XML Schema	101
F.1	Overview	101
F.2	UANodeSet	101
F.3	UANode	103
F.4	Reference	104
F.5	RolePermission	104
F.6	UAType	104
F.7	UAInstance	105
F.8	UAVariable	105
F.9	UAMethod	106
F.10	TranslationType	106
F.11	UADataType	107
F.12	DataTypeDefinition	108
F.13	DataTypeField	108
F.14	Variant	109
F.15	Example	110
F.16	UANodeSetChanges	112
F.17	NodesToAdd	113
F.18	ReferencesToChange	113
F.19	ReferenceToChange	114
F.20	NodesToDelete	114
F.21	NodeToDelete	114
F.22	UANodeSetChangesStatus	115
F.23	NodeSetStatusList	115
F.24	NodeSetStatus	115
Bibliography	117
Figure 1 – The OPC UA Stack Overview		15
Figure 2 – Encoding Integers in a binary stream		20
Figure 3 – Encoding Floating Points in a binary stream		20
Figure 4 – Encoding Strings in a binary stream		21
Figure 5 – Encoding GUIDs in a binary stream		22

Figure 6 – Encoding XmlElement in a binary stream	22
Figure 7 – A String NodeId.....	23
Figure 8 – A Two Byte NodeId	24
Figure 9 – A Four Byte NodeId.....	24
Figure 10 – Security handshake.....	55
Figure 11 – OPC UA Secure Conversation MessageChunk.....	63
Figure 12 – OPC UA Connection Protocol Message structure	72
Figure 13 – Client initiated OPC UA Connection Protocol connection.....	76
Figure 14 – Server initiated OPC UA Connection Protocol connection.....	76
Figure 15 – Closing a OPC UA Connection Protocol connection	77
Figure 16 – Scenarios for the HTTPS Transport.....	80
Figure 17 – Setting up Communication over a WebSocket	84
Table 1 – Built-in Data Types.....	16
Table 2 – Guid structure	17
Table 3 – Layout of Decimal	19
Table 4 – Supported Floating Point Types.....	20
Table 5 – NodeId components	22
Table 6 – NodeId DataEncoding values	23
Table 7 – Standard NodeId Binary DataEncoding.....	23
Table 8 – Two Byte NodeId Binary DataEncoding	24
Table 9 – Four Byte NodeId Binary DataEncoding.....	24
Table 10 – ExpandedNodeId Binary DataEncoding	25
Table 11 – DiagnosticInfo Binary DataEncoding.....	26
Table 12 – QualifiedName Binary DataEncoding.....	26
Table 13 – LocalizedText Binary DataEncoding	27
Table 14 – Extension Object Binary DataEncoding.....	28
Table 15 – Variant Binary DataEncoding.....	29
Table 16 – Data Value Binary DataEncoding.....	30
Table 17 – Sample OPC UA Binary Encoded structure.....	32
Table 18 – Sample OPC UA Binary Encoded Structure with optional fields	34
Table 19 – Sample OPC UA Binary Encoded Structure	35
Table 20 – XML Data Type Mappings for Integers.....	37
Table 21 – XML Data Type Mappings for Floating Points	37
Table 22 – Components of NodeId	39
Table 23 – Components of ExpandedNodeId	40
Table 24 – Components of Enumeration	44
Table 25 – JSON Object Definition for a NodeId	48
Table 26 – JSON Object Definition for an ExpandedNodeId	49
Table 27 – JSON Object Definition for a StatusCode	49
Table 28 – JSON Object Definition for a DiagnosticInfo	50
Table 29 – JSON Object Definition for a QualifiedName.....	50
Table 30 – JSON Object Definition for a LocalizedText	50

Table 31 – JSON Object Definition for an ExtensionObject	51
Table 32 – JSON Object Definition for a Variant	51
Table 33 – JSON Object Definition for a DataValue	52
Table 34 – JSON Object Definition for a Decimal	52
Table 35 – JSON Object Definition for a <i>Structure</i> with Optional Fields	53
Table 36 – JSON Object Definition for a Union	54
Table 37 – SecurityPolicy	56
Table 38 – Application Instance Certificate	57
Table 39 – Kerberos UserTokenPolicy	59
Table 40 – JWT UserTokenPolicy	59
Table 41 – JWT IssuerEndpointUrl Definition	60
Table 42 – Access Token Claims	61
Table 43 – OPC UA Secure Conversation Message header	63
Table 44 – Asymmetric algorithm Security header	64
Table 45 – Symmetric algorithm Security header	65
Table 46 – Sequence header	65
Table 47 – OPC UA Secure Conversation Message footer	66
Table 48 – OPC UA Secure Conversation Message abort body	67
Table 49 – OPC UA Secure Conversation OpenSecureChannel Service	68
Table 50 – PRF inputs for RSA based SecurityPolicies	70
Table 51 – Cryptography key generation parameters	70
Table 52 – OPC UA Connection Protocol Message header	72
Table 53 – OPC UA Connection Protocol Hello Message	73
Table 54 – OPC UA Connection Protocol Acknowledge Message	74
Table 55 – OPC UA Connection Protocol Error Message	74
Table 56 – OPC UA Connection Protocol ReverseHello Message	75
Table 57 – OPC UA Connection Protocol error codes	78
Table 58 – WebSocket Protocols Mappings	84
Table 59 – Well known addresses for Local Discovery Servers	85
Table A.1 – Identifiers assigned to Attributes	87
Table E.1 – SecuredApplication	94
Table E.2 – CertificateIdentifier	97
Table E.3 – Structured directory store	98
Table E.4 – CertificateStoreIdentifier	99
Table E.5 – CertificateList	99
Table E.6 – CertificateValidationOptions	100
Table F.1 – UANodeSet	102
Table F.2 – UANode	103
Table F.3 – Reference	104
Table F.4 – RolePermission	104
Table F.5 – UANodeSet Type Nodes	104
Table F.6 – UANodeSet Instance Nodes	105
Table F.7 – UAInstance	105

Table F.8 – UAVariable.....	106
Table F.9 – UAMethod.....	106
Table F.10 – TranslationType.....	107
Table F.11 – UADatatype.....	108
Table F.12 – DataTypeDefinition.....	108
Table F.13 – DataTypeField.....	109
Table F.14 – UANodeSetChanges.....	112
Table F.15 – NodesToAdd.....	113
Table F.16 – ReferencesToChange.....	113
Table F.17 – ReferencesToChange.....	114
Table F.18 – NodesToDelete.....	114
Table F.19 – ReferencesToChange.....	114
Table F.20 – UANodeSetChangesStatus.....	115
Table F.21 – NodeSetStatusList.....	115
Table F.22 – NodeSetStatus.....	116

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –**Part 6: Mappings****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 62541-6 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision.

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

- a) Encodings:
 - added JSON encoding for PubSub (non-reversible);
 - added JSON encoding for Client/Server (reversible);
 - added support for optional fields in structures;
 - added support for Unions.

- b) Transport mappings:
- added WebSocket secure connection – WSS;
 - added support for reverse connectivity;
 - added support for session-less service invocation in HTTPS.
- c) Deprecated Transport (missing support on most platforms):
- SOAP/HTTP with WS-SecureConversation (all encodings).
- d) Added mapping for JSON Web Token.
- e) Added support for Unions to NodeSet Schema.
- f) Added batch operations to add/delete nodes to/from NodeSet Schema.
- g) Added support for multi-dimensional arrays outside of Variants.
- h) Added binary representation for Decimal data types.
- i) Added mapping for an OAuth2 Authorization Framework.

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

FDIS	Report on voting
65E/718/FDIS	65E/734/RVD

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

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

Throughout this document and the other parts of IEC 62541, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in Clause 3 in one of the parts of the series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms and names* are also, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published under the general title *OPC Unified Architecture*, can be found on the IEC website.

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

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

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

OPC UNIFIED ARCHITECTURE –

Part 6: Mappings

1 Scope

This part of IEC 62541 specifies the OPC Unified Architecture (OPC UA) mapping between the security model described in IEC TR 62541-2, the abstract service definitions specified in IEC 62541-4, the data structures defined in IEC 62541-5 and the physical network protocols that can be used to implement the OPC UA specification.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TR 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security Model*

IEC 62541-3, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-7, *OPC Unified Architecture – Part 7: Profiles*

IEC 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

ISO 8601-1:2019, *Date and time – Representations for information interchange – Part 1: Basic rules*

XML Schema Part 2: XML Schema Part 2: Datatypes
<http://www.w3.org/TR/xmlschema-2/>

SOAP Part 1: SOAP Version 1.2 Part 1: Messaging Framework
<http://www.w3.org/TR/soap12-part1/>

SSL/TLS: RFC 5246 – The TLS Protocol Version 1.2
<http://tools.ietf.org/html/rfc5246.txt>

X.509 v3: ISO/IEC 9594-8 (ITU-T Rec. X.509), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

HTTP: RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1
<http://www.ietf.org/rfc/rfc2616.txt>

HTTPS: RFC 2818 – HTTP Over TLS
<http://www.ietf.org/rfc/rfc2818.txt>

Base64: RFC 3548 – The Base16, Base32, and Base64 Data Encodings
<http://www.ietf.org/rfc/rfc3548.txt>

X690: ISO/IEC 8825-1 (ITU-T Rec. X.690), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

IEEE-754: Standard for Floating-Point Arithmetic

HMAC: HMAC – Keyed-Hashing for Message Authentication
<http://www.ietf.org/rfc/rfc2104.txt>

PKCS #1: PKCS #1 – RSA Cryptography Specifications Version 2.0
<http://www.ietf.org/rfc/rfc2437.txt>

PKCS #12: PKCS #12 – Personal Information Exchange Syntax v1.1
<http://www.ietf.org/rfc/rfc7292.txt>

FIPS 180-4: Secure Hash Standard (SHS)
<https://csrc.nist.gov/publications/detail/fips/180/4/final>

FIPS 197: Advanced Encryption Standard (AES)
<https://csrc.nist.gov/publications/detail/fips/197/final>

UTF-8: UTF-8, a transformation format of ISO 10646
<http://www.ietf.org/rfc/rfc3629.txt>

RFC 3280: RFC 3280 – X.509 Public Key Infrastructure Certificate and CRL Profile
<http://www.ietf.org/rfc/rfc3280.txt>

RFC 4514: RFC 4514 – LDAP: String Representation of Distinguished Names
<http://www.ietf.org/rfc/rfc4514.txt>

NTP: RFC 1305 – Network Time Protocol (Version 3) Specification, Implementation and Analysis
<http://www.ietf.org/rfc/rfc1305.txt>

Kerberos: Web Services Security – Kerberos Token Profile 1.1
<http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf>

RFC 1738: RFC 1738 – Uniform Resource Locators (URL)
<http://www.ietf.org/rfc/rfc1738.txt>

RFC 2141: RFC 2141 – URN Syntax
<http://www.ietf.org/rfc/rfc2141.txt>

RFC 6455: RFC 6455 – The WebSocket Protocol
<http://www.ietf.org/rfc/rfc6455.txt>

RFC 7159: The JavaScript Object Notation (JSON) Data Interchange Format
<http://www.ietf.org/rfc/rfc7159.txt>

RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
<https://tools.ietf.org/rfc/rfc7523.txt>

RFC 6749: The OAuth 2.0 Authorization Framework
<http://www.ietf.org/rfc/rfc6749.txt>

OpenID-Core: OpenID Connect Core 1.0
http://openid.net/specs/openid-connect-core-1_0.html

OpenID-Discovery: OpenID Connect Discovery 1.0
https://openid.net/specs/openid-connect-discovery-1_0.html

RFC 6960: RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
<https://www.ietf.org/rfc/rfc6960.txt>