

# INTERNATIONAL STANDARD



OPC unified architecture – iTeh Standards  
Part 6: Mappings  
(<https://standards.iteh.ai>)  
Document Preview

[IEC 62541-6:2020](#)

<https://standards.iteh.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cabf6137/iec-62541-6-2020>



**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.

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

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

**About the IEC**

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

**About IEC publications**

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

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

[IEC 62541-6:2020](http://www.standards.iteh.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cab16137/iec-62541-6-2020)

<https://standards.iteh.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cab16137/iec-62541-6-2020>



IEC 62541-6

Edition 3.0 2020-07  
REDLINE VERSION

# INTERNATIONAL STANDARD



---

**OPC unified architecture – iTeh Standards**  
**Part 6: Mappings** (<https://standards.iteh.ai>)  
**Document Preview**

[IEC 62541-6:2020](#)

<https://standards.iteh.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cabf6137/iec-62541-6-2020>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

---

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-8665-4

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## CONTENTS

FOREWORD .....	8
1 Scope .....	11
2 Normative references .....	11
3 Terms, definitions, abbreviated terms and symbols.....	14
3.1 Terms and definitions.....	14
3.2 Abbreviated terms and symbols .....	15
4 Overview .....	16
5 Data encoding .....	17
5.1 General.....	17
5.1.1 Overview .....	17
5.1.2 Built-in Types .....	17
5.1.3 Guid .....	18
5.1.4 ByteString.....	19
5.1.5 ExtensionObject .....	19
5.1.6 Variant.....	19
5.1.7 Decimal .....	20
5.2 OPC UA Binary .....	21
5.2.1 General .....	21
5.2.2 Built-in Types .....	21
5.2.3 Decimal .....	32
5.2.4 Enumerations .....	32
5.2.5 Arrays.....	32
5.2.6 Structures.....	33
5.2.7 Structures with optional fields .....	35
5.2.8 Unions .....	37
5.2.9 Messages .....	38
5.3 OPC UA XML.....	39
5.3.1 Built-in Types .....	39
5.3.2 Decimal .....	45
5.3.3 Enumerations .....	45
5.3.4 Arrays.....	46
5.3.5 Structures.....	46
5.3.6 Structures with optional fields .....	47
5.3.7 Unions .....	47
5.3.8 Messages .....	48
5.4 OPC UA JSON.....	48
5.4.1 General .....	48
5.4.2 Built-in Types .....	49
5.4.3 Decimal .....	54
5.4.4 Enumerations .....	54
5.4.5 Arrays.....	54
5.4.6 Structures.....	55
5.4.7 Structures with optional fields .....	55
5.4.8 Unions .....	56
5.4.9 Messages .....	56
6 Message SecurityProtocols .....	57

6.1	Security handshake .....	57
6.2	Certificates .....	59
6.2.1	General .....	59
6.2.2	Application Instance Certificate.....	59
<del>6.2.3</del>	<del>Signed Software Certificate .....</del>	<del>61</del>
6.2.3	Certificate Chains .....	61
6.3	Time synchronization .....	61
6.4	UTC and International Atomic Time (TAI).....	62
6.5	Issued User Identity Tokens.....	62
6.5.1	Kerberos.....	62
6.5.2	JSON Web Token (JWT).....	63
6.5.3	OAuth2 .....	63
6.6	WS Secure Conversation .....	65
6.7	OPC UA Secure Conversation .....	70
6.7.1	Overview .....	70
6.7.2	MessageChunk structure .....	70
6.7.3	MessageChunks and error handling.....	75
6.7.4	Establishing a SecureChannel .....	75
6.7.5	Deriving keys.....	77
6.7.6	Verifying Message security .....	79
7	TransportProtocols .....	80
7.1	OPC UA <del>TCP</del> Connection Protocol.....	80
7.1.1	Overview .....	80
7.1.2	Message structure .....	80
7.1.3	Establishing a connection .....	84
7.1.4	Closing a connection .....	87
7.1.5	Error handling.....	87
7.2	OPC UA TCP.....	91
7.3	SOAP/HTTP.....	91
7.4	OPC UA HTTPS.....	93
7.4.1	Overview .....	93
7.4.2	Session-less Services.....	95
7.4.3	XML Encoding .....	95
7.4.4	OPC UA Binary Encoding .....	96
7.4.5	JSON Encoding .....	97
7.5	WebSockets.....	97
7.5.1	Overview .....	97
7.5.2	Protocol Mapping.....	98
7.5.3	Security .....	98
7.6	Well known addresses .....	99
8	Normative Contracts .....	100
8.1	OPC Binary Schema .....	100
8.2	XML Schema and WSDL.....	100
8.3	Information Model Schema.....	100
8.4	Formal definition of UA Information Model.....	100
8.5	Constants .....	100
8.6	DataType encoding.....	100
8.7	Security configuration .....	100
Annex A	(normative) Constants.....	101

A.1	Attribute Ids .....	101
A.2	Status Codes .....	101
A.3	Numeric Node Ids .....	102
Annex B	(normative) OPC UA Nodeset .....	103
Annex C	(normative) Type declarations for the OPC UA native Mapping .....	104
Annex D	(normative) WSDL for the XML Mapping .....	105
D.1	XML Schema .....	105
D.2	WDSL Port Types .....	105
D.3	WSDL Bindings .....	105
Annex E	(normative) Security settings management .....	106
E.1	Overview .....	106
E.2	SecuredApplication .....	107
E.3	CertificateIdentifier .....	110
E.4	CertificateStoreIdentifier .....	112
E.5	CertificateList .....	113
E.6	CertificateValidationOptions .....	113
Annex F	(normative) Information Model XML Schema .....	115
F.1	Overview .....	115
F.2	UANodeSet .....	115
F.3	UANode .....	117
F.4	Reference .....	118
F.5	RolePermission .....	118
F.6	UAType .....	118
F.7	UAInstance .....	119
F.8	UAVariable .....	119
F.9	UAMethod .....	120
F.10	TranslationType .....	121
F.11	UADataType .....	122
F.12	DataTypeDefinition .....	122
F.13	DataTypeField .....	123
F.14	Variant .....	124
F.15	Example .....	125
F.16	UANodeSetChanges .....	127
F.17	NodesToAdd .....	128
F.18	ReferencesToChange .....	128
F.19	ReferenceToChange .....	129
F.20	NodesToDelete .....	129
F.21	NodeToDelete .....	129
F.22	UANodeSetChangesStatus .....	130
F.23	NodeSetStatusList .....	130
F.24	NodeSetStatus .....	131
Bibliography	.....	132
Figure 1	– The OPC UA Stack Overview .....	17
Figure 2	– Encoding Integers in a binary stream .....	21
Figure 3	– Encoding Floating Points in a binary stream .....	22
Figure 4	– Encoding Strings in a binary stream .....	22

Figure 5 – Encoding Guid in a binary stream .....	23
Figure 6 – Encoding XmlElement in a binary stream .....	24
Figure 7 – A String NodeId .....	25
Figure 8 – A Two Byte NodeId .....	26
Figure 9 – A Four Byte NodeId .....	26
Figure 10 – Security handshake .....	57
Figure 11 – OPC UA Secure Conversation MessageChunk .....	70
Figure 12 – OPC UA <del>TCP</del> Connection Protocol Message structure .....	80
Figure 13 – Client initiated OPC UA Connection Protocol connection .....	86
Figure 14 – Server initiated OPC UA Connection Protocol connection .....	86
Figure 15 – Closing a OPC UA <del>TCP</del> Connection Protocol connection .....	87
Figure 16 – Scenarios for the HTTPS Transport .....	94
Figure 17 – Setting up Communication over a WebSocket .....	98
Table 1 – Built-in Data Types .....	18
Table 2 – Guid structure .....	18
Table 3 – Layout of Decimal .....	20
Table 4 – Supported Floating Point Types .....	22
Table 5 – NodeId components .....	24
Table 6 – NodeId DataEncoding values .....	25
Table 7 – Standard NodeId Binary DataEncoding .....	25
Table 8 – Two Byte NodeId Binary DataEncoding .....	26
Table 9 – Four Byte NodeId Binary DataEncoding .....	26
Table 10 – ExpandedNodeId Binary DataEncoding .....	27
Table 11 – DiagnosticInfo Binary DataEncoding .....	28
Table 12 – QualifiedName Binary DataEncoding .....	28
Table 13 – LocalizedText Binary DataEncoding .....	29
Table 14 – Extension Object Binary DataEncoding .....	30
Table 15 – Variant Binary DataEncoding .....	31
Table 16 – Data Value Binary DataEncoding .....	32
Table 17 – Sample OPC UA Binary Encoded structure .....	34
Table 18 – Sample OPC UA Binary Encoded Structure with optional fields .....	36
Table 19 – Sample OPC UA Binary Encoded Structure .....	37
Table 20 – XML Data Type Mappings for Integers .....	39
Table 21 – XML Data Type Mappings for Floating Points .....	39
Table 22 – Components of NodeId .....	41
Table 23 – Components of ExpandedNodeId .....	42
Table 24 – Components of Enumeration .....	46
Table 25 – JSON Object Definition for a NodeId .....	50
Table 26 – JSON Object Definition for an ExpandedNodeId .....	51
Table 27 – JSON Object Definition for a StatusCode .....	51
Table 28 – JSON Object Definition for a DiagnosticInfo .....	52
Table 29 – JSON Object Definition for a QualifiedName .....	52

Table 30 – JSON Object Definition for a LocalizedText .....	52
Table 31 – JSON Object Definition for an ExtensionObject .....	53
Table 32 – JSON Object Definition for a Variant .....	53
Table 33 – JSON Object Definition for a DataValue .....	54
Table 34 – JSON Object Definition for a Decimal .....	54
Table 35 – JSON Object Definition for a <i>Structure</i> with Optional Fields .....	55
Table 36 – JSON Object Definition for a Union .....	56
Table 37 – SecurityPolicy .....	58
Table 38 – Application Instance Certificate .....	60
Table 39 – Kerberos UserTokenPolicy .....	62
Table 40 – JWT UserTokenPolicy .....	63
Table 41 – JWT IssuerEndpointUrl Definition .....	63
Table 42 – Access Token Claims .....	64
Table 43 – OPC UA Secure Conversation Message header .....	71
Table 44 – Asymmetric algorithm Security header .....	72
Table 45 – Symmetric algorithm Security header .....	73
Table 46 – Sequence header .....	73
Table 47 – OPC UA Secure Conversation Message footer .....	74
Table 48 – OPC UA Secure Conversation Message abort body .....	75
Table 49 – OPC UA Secure Conversation OpenSecureChannel Service .....	76
Table 50 – PRF inputs for RSA based SecurityPolicies .....	78
Table 51 – Cryptography key generation parameters .....	78
Table 52 – OPC UA <del>TCP</del> Connection Protocol Message header .....	81
Table 53 – OPC UA <del>TCP</del> Connection Protocol Hello Message .....	82
Table 54 – OPC UA <del>TCP</del> Connection Protocol Acknowledge Message .....	83
Table 55 – OPC UA <del>TCP</del> Connection Protocol Error Message .....	83
Table 56 – OPC UA Connection Protocol ReverseHello Message .....	84
Table 57 – OPC UA Connection Protocol error codes .....	89
Table 58 – WebSocket Protocols Mappings .....	98
Table 59 – Well known addresses for Local Discovery Servers .....	99
Table A.1 – Identifiers assigned to Attributes .....	101
Table E.1 – SecuredApplication .....	108
Table E.2 – CertificateIdentifier .....	111
Table E.3 – Structured directory store .....	112
Table E.4 – CertificateStoreIdentifier .....	113
Table E.5 – CertificateList .....	113
Table E.6 – CertificateValidationOptions .....	114
Table F.1 – UANodeSet .....	116
Table F.2 – UANode .....	117
Table F.3 – Reference .....	118
Table F.4 – RolePermission .....	118
Table F.5 – UANodeSet Type Nodes .....	118
Table F.6 – UANodeSet Instance Nodes .....	119



Table F.7 – UAInstance .....	119
Table F.8 – UAVariable .....	120
Table F.9 – UAMethod .....	120
Table F.10 – TranslationType .....	121
Table F.11 – UADatatype .....	122
Table F.12 – DataTypeDefinition .....	122
Table F.13 – DataTypeField .....	123
Table F.14 – UANodeSetChanges .....	127
Table F.15 – NodesToAdd .....	128
Table F.16 – ReferencesToChange .....	129
Table F.17 – ReferencesToChange .....	129
Table F.18 – NodesToDelete .....	129
Table F.19 – ReferencesToChange .....	130
Table F.20 – UANodeSetChangesStatus .....	130
Table F.21 – NodeSetStatusList .....	131
Table F.22 – NodeSetStatus .....	131

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[IEC 62541-6:2020](#)

<https://standards.itih.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cabf6137/iec-62541-6-2020>

## 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.

**This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.**

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.**

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[IEC 62541-6:2020](#)

<https://standards.itih.ai/catalog/standards/iec/90d7843d-e271-49a5-850c-e251cabf6137/iec-62541-6-2020>

## 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, ~~described~~ ~~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 1: XML Schema Part 1: Structures~~

~~<http://www.w3.org/TR/xmlschema-1/>~~

~~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/>~~

~~SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts~~

~~<http://www.w3.org/TR/soap12-part2/>~~

~~XML Encryption: XML Encryption Syntax and Processing~~

~~<http://www.w3.org/TR/xmlenc-core/>~~

~~XML Signature: XML Signature Syntax and Processing~~

~~<http://www.w3.org/TR/xmlsig-core/>~~

~~WS Security: SOAP Message Security 1.1~~

~~<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>~~

~~WS Addressing: Web Services Addressing (WS-Addressing)~~

~~<http://www.w3.org/Submission/ws-addressing/>~~

~~WS Trust: WS Trust 1.3~~

~~<http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html>~~

~~WS Secure Conversation: WS Secure Conversation 1.3~~

~~<http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html>~~

~~WS Security Policy: WS Security Policy 1.2~~

~~<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html>~~

~~SSL/TLS: RFC 5246 — The TLS Protocol Version 1.2~~

~~<http://tools.ietf.org/html/rfc5246.txt>~~

~~X509: X.509 Public Key Certificate Infrastructure~~

~~<http://www.itu.int/rec/T-REC-X.509-200003-I/e>~~

~~WS-I Basic Profile 1.1: WS-I Basic Profile Version 1.1~~

~~<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>~~

~~WS-I Basic Security Profile 1.1: WS-I Basic Security Profile Version 1.1~~

~~<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>~~

~~HTTP: RFC 2616 — Hypertext Transfer Protocol — HTTP/1.1~~

~~<http://www.ietf.org/rfc/rfc2616.txt>~~

~~Base64: RFC 3548 — The Base16, Base32, and Base64 Data Encodings~~

~~<http://www.ietf.org/rfc/rfc3548.txt>~~

~~X.690: ITU-T X.690 — Basic (BER), Canonical (CER) and Distinguished (DER) Encoding Rules~~

~~<http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>~~

~~IEEE 754: Standard for Binary Floating-Point Arithmetic~~

~~<http://grouper.ieee.org/groups/754/>~~

~~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>~~

~~FIPS 180-2: Secure Hash Standard (SHA)~~

~~<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>~~

~~FIPS 197: Advanced Encryption Standard (AES)~~

~~<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>~~

~~UTF8: UTF-8, a transformation format of ISO 10646~~

~~<http://tools.ietf.org/html/rfc3629>~~