

INTERNATIONAL STANDARD

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



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2025 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 Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

CONTENTS

FOREWORD	8
1 Scope	10
2 Normative references	10
3 Terms, definitions and abbreviated terms	12
3.1 Terms and definitions	12
3.2 Abbreviated terms	14
4 Overview	14
5 Data encoding	15
5.1 General	15
5.1.1 Overview	15
5.1.2 Built-in Types	15
5.1.3 Guid	17
5.1.4 DateTime	17
5.1.5 ByteString	18
5.1.6 Number, Integer and UInteger	18
5.1.7 Structures and Unions	18
5.1.8 ExtensionObject	18
5.1.9 Variant	19
5.1.10 Decimal	19
5.1.11 Null, Empty and Zero-Length Arrays	20
5.1.12 QualifiedName, NodeId and ExpandedNodeId String Encoding	20
5.1.13 Name Encoding Rules	22
5.2 OPC UA Binary	23
5.2.1 General	23
5.2.2 Built-in Types	23
5.2.3 Decimal	34
5.2.4 Enumerations	34
5.2.5 Arrays	34
5.2.6 Structures	35
5.2.7 Structures with optional fields	38
5.2.8 Unions	40
5.2.9 Messages	43
5.3 OPC UA XML	43
5.3.1 Built-in Types	43
5.3.2 Decimal	48
5.3.3 Enumerations	49
5.3.4 Arrays	49
5.3.5 Structures	50
5.3.6 Structures with optional fields	50
5.3.7 Unions	51
5.3.8 Messages	51
5.4 OPC UA JSON	51
5.4.1 General	51
5.4.2 Built-in Types	52
5.4.3 Decimal	57
5.4.4 Enumerations	57

5.4.5	Arrays.....	58
5.4.6	Structures.....	58
5.4.7	Structures with optional fields	59
5.4.8	Unions	60
5.4.9	Messages	61
6	Message SecurityProtocols	61
6.1	Security handshake	61
6.2	Certificates	63
6.2.1	General	63
6.2.2	Application Instance Certificate	63
6.2.3	User Certificates.....	65
6.2.4	Issuer (CA) Certificates	65
6.2.5	Certificate Revocation List (CRL).....	65
6.2.6	Certificate Chains	66
6.3	Time synchronization	66
6.4	UTC and International Atomic Time (TAI).....	67
6.5	Issued User Identity Tokens.....	67
6.5.1	Kerberos.....	67
6.5.2	JSON Web Token (JWT).....	67
6.5.3	OAuth2	68
6.6	WS Secure Conversation	70
6.7	OPC UA Secure Conversation	70
6.7.1	Overview	70
6.7.2	MessageChunk structure	71
6.7.3	MessageChunks and error handling.....	76
6.7.4	Establishing a SecureChannel	77
6.7.5	Deriving keys.....	78
6.7.6	Verifying Message Security	80
6.8	Elliptic Curve Cryptography (ECC)	81
6.8.1	Secure Channel Handshake	81
6.8.2	UserIdentityToken Encryption	85
6.8.3	ECC Encrypted Secret.....	86
7	TransportProtocols	87
7.1	OPC UA Connection Protocol	87
7.1.1	Overview	87
7.1.2	Message structure	88
7.1.3	Establishing a connection	91
7.1.4	Closing a connection	93
7.1.5	Error handling.....	94
7.2	OPC UA TCP	96
7.3	SOAP/HTTP.....	96
7.4	OPC UA HTTPS.....	96
7.4.1	Overview	96
7.4.2	Session-less Services.....	98
7.4.3	XML Encoding	98
7.4.4	OPC UA Binary Encoding	99
7.4.5	JSON Encoding	99
7.5	WebSockets.....	100
7.5.1	Overview	100

7.5.2	Protocol Mapping.....	101
7.5.3	Security	101
7.6	Well known addresses	102
8	Normative Contracts	102
8.1	OPC Binary Schema	102
8.2	XML Schema and WSDL	102
8.3	Information Model Schema.....	102
8.4	Formal definition of UA Information Model	103
8.5	Constants	103
8.6	DataType encoding	103
8.7	Security configuration	103
Annex A	(normative) Constants.....	104
A.1	Attribute Ids	104
A.2	Status Codes	104
A.3	Numeric Node Ids	105
A.4	Media Types	106
Annex B	(normative) OPC UA NodeSet.....	107
Annex C	(normative) Type declarations for the OPC UA native Mapping.....	108
Annex D	(normative) WSDL for the XML Mapping	109
D.1	XML Schema	109
D.2	WSDL Port Types	109
D.3	WSDL Bindings.....	109
Annex E	(informative) Security settings management.....	110
E.1	Overview	110
E.2	SecuredApplication	111
E.3	CertificateIdentifier	115
E.4	CertificateStoreIdentifier	116
E.5	CertificateList.....	117
E.6	CertificateValidationOptions.....	117
Annex F	(normative) Information Model XML Schema	119
F.1	Overview	119
F.2	UANodeSet.....	119
F.3	UANode	122
F.4	Reference	123
F.5	RolePermission.....	124
F.6	UAType.....	124
F.7	UAInstance	124
F.8	UAVariable	125
F.9	UAMethod.....	125
F.10	TranslationType	126
F.11	UADatatype	127
F.12	DataTypeDefinition	128
F.13	DataTypeField	129
F.14	Variant.....	131
F.15	Example	131
F.16	UANodeSetChanges	133
F.17	NodesToAdd.....	134
F.18	ReferencesToChange	135

F.19	ReferenceToChange	135
F.20	NodesToDelete	135
F.21	NodeToDelete	136
F.22	UANodeSetChangesStatus	136
F.23	NodeSetStatusList	137
F.24	NodeSetStatus	137
	Bibliography	138
Figure 1	– The OPC UA Stack Overview	15
Figure 2	– Encoding Integers in a binary stream	24
Figure 3	– Encoding Floating Points in a binary stream	24
Figure 4	– Encoding Strings in a binary stream	25
Figure 5	– Encoding Guids in a binary stream	26
Figure 6	– Encoding XmlElement in a binary stream	26
Figure 7	– A String NodeId	27
Figure 8	– A Two Byte NodeId	28
Figure 9	– A Four Byte NodeId	28
Figure 10	– Security handshake when Creating a Session	61
Figure 11	– MessageChunk for Unauthenticated Encryption Algorithms	71
Figure 12	– MessageChunk for Authenticated Encryption Algorithms	71
Figure 13	– ECC Key Negotiation	81
Figure 14	– Signing and Encryption with Authenticated Encryption	84
Figure 15	– Signing and Encryption with Unauthenticated Encryption	84
Figure 16	– ECC CreateSession/ActivateSession Handshake	85
Figure 17	– OPC UA Connection Protocol Message structure	88
Figure 18	– Client initiated OPC UA Connection Protocol connection	92
Figure 19	– Server initiated OPC UA Connection Protocol connection	92
Figure 20	– Closing a OPC UA Connection Protocol connection	94
Figure 21	– Scenarios for the HTTPS Transport	97
Figure 22	– Setting up Communication over a WebSocket	100
Table 1	– Built-in Data Types	16
Table 2	– Guid structure	17
Table 3	– Layout of Decimal	20
Table 4	– Additional ABNF Core Rules	21
Table 5	– ABNF Description for a NodeId	21
Table 6	– ABNF Description for a ExpandedNodeId	22
Table 7	– ABNF Description for a QualifiedName	22
Table 8	– Examples of XML Encoded Names	23
Table 9	– Supported Floating Point Types	24
Table 10	– NodeId components	26
Table 11	– NodeId DataEncoding values	27
Table 12	– Standard NodeId Binary DataEncoding	27
Table 13	– Two Byte NodeId Binary DataEncoding	28

Table 14 – Four Byte NodeId Binary DataEncoding	28
Table 15 – ExpandedNodeId Binary DataEncoding	29
Table 16 – DiagnosticInfo Binary DataEncoding	30
Table 17 – QualifiedName Binary DataEncoding	30
Table 18 – LocalizedText Binary DataEncoding	31
Table 19 – Extension Object Binary DataEncoding	32
Table 20 – Variant Binary DataEncoding	33
Table 21 – Data Value Binary DataEncoding	34
Table 22 – Inline Matrix DataEncoding	35
Table 23 – Sample OPC UA Binary Encoded structure	36
Table 24 – DataTypeDefinition for "Type1" from Sample	37
Table 25 – DataTypeDefinition for "Type2" from Sample	38
Table 26 – Sample OPC UA Binary Encoded Structure with optional fields	39
Table 27 – Sample OPC UA Binary Encoded Structure	41
Table 28 – XML Data Type Mappings for Integers	43
Table 29 – XML Data Type Mappings for Floating Points	43
Table 30 – Components of Enumeration	49
Table 31 – JSON Object Definition for a NodeId	53
Table 32 – JSON Object Definition for an ExpandedNodeId	54
Table 33 – JSON Object Definition for a StatusCode	54
Table 34 – JSON Object Definition for a DiagnosticInfo	55
Table 35 – JSON Object Definition for a QualifiedName	55
Table 36 – JSON Object Definition for a LocalizedText	56
Table 37 – JSON Object Definition for an ExtensionObject	56
Table 38 – JSON Object Definition for a Variant	56
Table 39 – JSON Object Definition for a DataValue	57
Table 40 – JSON Object Definition for a Decimal	57
Table 41 – JSON Encoding Rules for Structures	58
Table 42 – JSON Object Definition for a Structures with Optional Fields	59
Table 43 – JSON Encoding Rules for Structures with Optional Fields	59
Table 44 – JSON Object Definition for a Union	60
Table 45 – SecurityPolicy	62
Table 46 – Application Instance Certificate	63
Table 47 – User Certificate	65
Table 48 – Issuer Certificate	65
Table 49 – Certificate Revocation List Extensions	66
Table 50 – JWT UserTokenPolicy	67
Table 51 – JWT IssuerEndpointUrl Definition	68
Table 52 – Access Token Claims	69
Table 53 – OPC UA Secure Conversation Message Header	72
Table 54 – Asymmetric algorithm Security header	73
Table 55 – Symmetric algorithm Security header	74
Table 56 – Sequence header	74

Table 57 – Message Footer for Unauthenticated Encryption Algorithms	75
Table 58 – Message Footer for Authenticated Encryption Algorithms	76
Table 59 – OPC UA Secure Conversation Message abort body.....	76
Table 60 – OPC UA Secure Conversation OpenSecureChannel Service	77
Table 61 – PRF inputs for RSA based SecurityPolicies	79
Table 62 – Cryptography key generation parameters	79
Table 63 – Deriving Client Keys from Keying Material	83
Table 64 – Deriving Server Keys from Keying Material.....	83
Table 65 – Creating a Mask for the Initialization Vector	85
Table 66 – Additional Header Key Names	86
Table 67 – Deriving Keys from Keying Material	87
Table 68 – OPC UA Connection Protocol Message header	88
Table 69 – OPC UA Connection Protocol Hello Message	89
Table 70 – OPC UA Connection Protocol Acknowledge Message.....	90
Table 71 – OPC UA Connection Protocol Error Message	90
Table 72 – OPC UA Connection Protocol ReverseHello Message	91
Table 73 – Client and Server Handshake during Reverse Connect.....	93
Table 74 – OPC UA Connection Protocol error codes	95
Table 75 – WebSocket Protocols Mappings	101
Table 76 – Well known addresses for Local Discovery Servers	102
Table A.1 – Identifiers assigned to Attributes	104
Table A.2 – Media Types Assigned to OPC UA Document Formats.....	106
Table E.1 – SecuredApplication	112
Table E.2 – CertificateIdentifier.....	115
Table E.3 – Structured directory store.....	116
Table E.4 – CertificateStoreIdentifier	117
Table E.5 – CertificateList.....	117
Table E.6 – CertificateValidationOptions	118
Table F.1 – UANodeSet	120
Table F.2 – UANode	122
Table F.3 – Reference	123
Table F.4 – RolePermission	124
Table F.5 – UANodeSet Type Nodes	124
Table F.6 – UANodeSet Instance Nodes	124
Table F.7 – UAInstance	125
Table F.8 – UAVariable.....	125
Table F.9 – UAMethod	126
Table F.10 – TranslationType	127
Table F.11 – UADatatype.....	128
Table F.12 – DataTypeDefinition.....	129
Table F.13 – StructureType Enumeration Mapping.....	129
Table F.14 – DataTypeField.....	130
Table F.15 – UANodeSetChanges	134

Table F.16 – NodesToAdd	134
Table F.17 – ReferencesToChange.....	135
Table F.18 – ReferencesToChange.....	135
Table F.19 – NodesToDelete	136
Table F.20 – ReferencesToChange.....	136
Table F.21 – UANodeSetChangesStatus.....	136
Table F.22 – NodeSetStatusList.....	137
Table F.23 – NodeSetStatus	137

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had no received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

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. It is an International Standard.

This fourth edition cancels and replaces the third edition published in 2020. This edition constitutes a technical revision.

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

- a) addition of support for ECC to UA Secure Conversation;
- b) use of the AuthorityKeyIdentifier extension in Certificate Revocation Lists;
- c) enhancement of JSON mapping of Unions;
- d) addition of Decimal data type encoding.
- e) description of ECC keyUsage rules;

- f) addition of Media assigned by IANA to UANodeSet definition;
- g) addition of requirements for user and issuer Certificates;
- h) addition of rules which specify what happens when DateTime precision is lost;
- i) addition of rules to allow for the truncation of strings containing embedded nulls.
- j) definition of a normative string representation for NodeId, ExpandedNodeId and QualifiedName for JSON mapping.
- k) requirement that TAI times be converted to UTC;
- l) new possibility to omit Symbol if unknown in JSON encoding;
- m) addition of fields needed to support RolePermissions to the UANodeSet.

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

Draft	Report on voting
65E/1063/CDV	65E/1131/RVC

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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

Italics are used to denote a defined term or definition that appears in the "Terms and definitions" clause in one of the parts of the IEC 62541 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, 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 in 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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

1 Scope

This part of IEC 62541 specifies the mapping between the security model described in IEC 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 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 62541-1, *OPC Unified Architecture - Part 1: Overview and Concepts*

IEC 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*

IEC 62541-18, *OPC Unified Architecture - Part 18: Role-Based Security*

ISO/IEC 60559, IEEE 754, *Information technology - Microprocessor Systems - Floating-Point arithmetic*

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

Recommendation ITU-T X.200 | ISO/IEC 7498-1, *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model*

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

Recommendation ITU-T X.509 | ISO/IEC 9594-8, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*

IETF RFC 2104, Krawczyk H., Bellare M. and Canetti R., "HMAC: Keyed-Hashing for Message Authentication", February 1997, available at <http://www.ietf.org/rfc/rfc2104.txt>

IETF RFC 2818, Rescorla E., "HTTPS, HTTP Over TLS", May 2000, available at <http://www.ietf.org/rfc/rfc2818.txt>

IETF RFC 3629, Yergeau F., "UTF-8, a transformation format of ISO 10646", November 2003, available at <https://datatracker.ietf.org/doc/html/rfc3629>

IETF RFC 3986, Berners-Lee T., Fielding R. and Masinter L., “Uniform Resource Identifier (URI): Generic Syntax”, January 2005, available at <https://datatracker.ietf.org/doc/html/rfc3986>

IETF RFC 4648, Josefsson S., “The Base16, Base32, and Base64 Data Encodings”, October 2006, available at <https://datatracker.ietf.org/doc/html/rfc4648>

IETF RFC 7230, Fielding R. and Reschke J., “HTTP, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”, June 2014, available at <https://datatracker.ietf.org/doc/html/rfc7230>

IETF RFC 4514, Zeilenga K., “LDAP: String Representation of Distinguished Names”, June 2006, available at <https://datatracker.ietf.org/doc/html/rfc4514>

IETF RFC 5234, Crocker D, Overell P., “Augmented BNF for Syntax Specifications: ABNF”, January 2008, available at <https://datatracker.ietf.org/doc/html/rfc5234>

IETF RFC 5280, Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W., “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008, available at <https://datatracker.ietf.org/doc/html/rfc5280>

IETF RFC 5392, Chen M., Zhang R., Duan X., “OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering”, January 2009, available at <https://datatracker.ietf.org/doc/html/rfc5392>

IETF RFC 5869, Krawczyk H, Eronen P., “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, May 2010, available at <https://datatracker.ietf.org/doc/html/rfc5869>

IETF RFC 5905, Mills D., Delaware U., Martin J., Burbank J., Kasch W., “Network Time Protocol Version 4: Protocol and Algorithms Specification”, June 2010, available at <https://datatracker.ietf.org/doc/html/rfc5905>

IETF RFC 6455, Fette I., Melnikov A., “The WebSocket Protocol”, December 2011, available at <https://datatracker.ietf.org/doc/html/rfc6455>

IETF RFC 6749, Hardt D., “The OAuth 2.0 Authorization Framework”, October 2012, available at <https://datatracker.ietf.org/doc/html/rfc6749>

IETF RFC 6750, Jones M., Hardt D., “The OAuth 2.0 Authorization Framework: Bearer Token Usage”, October 2012, available at <https://datatracker.ietf.org/doc/html/rfc6750>

IETF RFC 6960, Santesson S., Myers M., Ankney R., Malpani A., Galperin S. and Adams C., “X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP”, June 2013, available at <https://datatracker.ietf.org/doc/html/rfc6960>

IETF RFC 7292, Moriarty K., Nystrom M., Parkinson S., Rusch A. and Scott M., “PKCS #12: Personal Information Exchange Syntax v1.1”, July 2014, available at <https://datatracker.ietf.org/doc/html/rfc7292>

IETF RFC 7523, Jones M., Campbell B., Mortimore C., “JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants”, May 2015, available at <https://datatracker.ietf.org/doc/html/rfc7523>

IETF RFC 8017, Moriarty K., Kaliski B., Jonsson J., “PKCS #1, RSA Cryptography Specifications Version 2.2”, November 2016, available at <https://datatracker.ietf.org/doc/html/rfc8017>

IETF RFC 8141, Saint-Andre P., Klensin J. “Uniform Resource Names (URNs)”, April 2017, available at <https://datatracker.ietf.org/doc/html/rfc8141>

IETF RFC 8259, Bray T., “The JavaScript Object Notation (JSON) Data Interchange Format”, December 2017, available at <https://datatracker.ietf.org/doc/html/rfc8259>

IETF RFC 8422, Nir Y., Josefsson S., Pegourie-Gonnard M., “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier”, August 2018, available at <https://datatracker.ietf.org/doc/html/rfc8422>

IETF RFC 8446, Rescorla E., “The Transport Layer Security (TLS) Protocol Version 1.3”, August 2018, available at <https://datatracker.ietf.org/doc/html/rfc8446>

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

FIPS 197, Advanced Encryption Standard (AES), available at <https://www.nist.gov/publications/advanced-encryption-standard-aes>

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

WS Addressing, Web Services Addressing (WS-Addressing)
<http://www.w3.org/Submission/ws-addressing/>

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

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

SemVer, Semantic Versioning 2.0.0
<https://semver.org/spec/v2.0.0.html>

Bibliography

IEC 62541-21, *OPC Unified Architecture - Part 21: Device Onboarding*
