



IEC 62541-6

Edition 3.0 2020-07
REDLINE VERSION

INTERNATIONAL STANDARD



OPC unified architecture – Part 6: Mappings

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
6.2.3	Signed Software Certificate	59
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 TCP 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	WSDL 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 Guids 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 TCP 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 TCP 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 TCP Connection Protocol Message header	81
Table 53 – OPC UA TCP Connection Protocol Hello Message	82
Table 54 – OPC UA TCP Connection Protocol Acknowledge Message	83
Table 55 – OPC UA TCP 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

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.

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>~~

~~X.509: 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>~~

~~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)~~

~~<http://www.ietf.org/rfc/rfc1305.txt>~~

~~Kerberos: WS Security Kerberos Token Profile 1.1~~

~~<http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf>~~

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>

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

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>

SOMMAIRE

AVANT-PROPOS	124
1 Domaine d'application	127
2 Références normatives	127
3 Termes, définitions, termes abrégés et symboles	129
3.1 Termes et définitions	129
3.2 Termes abrégés et symboles	130
4 Vue d'ensemble	130
5 Codage de données	132
5.1 Généralités	132
5.1.1 Vue d'ensemble	132
5.1.2 Types intégrés	132
5.1.3 Guid	133
5.1.4 ByteString	134
5.1.5 ExtensionObject	134
5.1.6 Variant	135
5.1.7 Decimal	135
5.2 Codage OPC UA binaire	136
5.2.1 Généralités	136
5.2.2 Types intégrés	137
5.2.3 Décimaux	147
5.2.4 Enumérations	147
5.2.5 Matrices	147
5.2.6 Structures	148
5.2.7 Structures avec champs facultatifs	150
5.2.8 Unions	152
5.2.9 Messages	153
5.3 Codage OPC UA XML	154
5.3.1 Types intégrés	154
5.3.2 Décimaux	161
5.3.3 Enumérations	161
5.3.4 Matrices	162
5.3.5 Structures	162
5.3.6 Structures avec champs facultatifs	162
5.3.7 Unions	163
5.3.8 Messages	163
5.4 Codage OPC UA JSON	164
5.4.1 Généralités	164
5.4.2 Types intégrés	164
5.4.3 Décimaux	170
5.4.4 Enumérations	171
5.4.5 Matrices	171
5.4.6 Structures	171
5.4.7 Structures avec champs facultatifs	172
5.4.8 Unions	173
5.4.9 Messages	173
6 SecurityProtocols des messages	173

6.1	Protocole d'établissement de liaison de sécurité	173
6.2	Certificats	175
6.2.1	Généralités	175
6.2.2	Certificat d'instance d'application	176
6.2.3	Chaînes de Certificats	177
6.3	Synchronisation horaire	177
6.4	Temps universel coordonné (UTC) et Temps atomique international (TAI)	177
6.5	Jetons d'identité utilisateur émis	178
6.5.1	Kerberos	178
6.5.2	JWT (JSON Web Token)	178
6.5.3	OAuth2	179
6.6	Conversation sécurisée WS	181
6.7	Conversation OPC UA sécurisée	181
6.7.1	Vue d'ensemble	181
6.7.2	Structure de MessageChunk	182
6.7.3	MessageChunks et traitement d'erreurs	186
6.7.4	Etablissement d'un SecureChannel	186
6.7.5	Dérivation des clés	188
6.7.6	Vérification de la sécurité d'un message	189
7	TransportProtocols	190
7.1	Protocole de connexion OPC UA	190
7.1.1	Vue d'ensemble	190
7.1.2	Structure de message	191
7.1.3	Etablissement d'une connexion	194
7.1.4	Fermeture d'une connexion	196
7.1.5	Traitement d'erreurs	196
7.2	OPC UA TCP	198
7.3	SOAP/HTTP	198
7.4	OPC UA HTTPS	198
7.4.1	Vue d'ensemble	198
7.4.2	Services sans Session	200
7.4.3	Codage XML	200
7.4.4	Codage OPC UA binaire	201
7.4.5	Codage JSON	202
7.5	WebSockets	202
7.5.1	Vue d'ensemble	202
7.5.2	Mapping de protocole	203
7.5.3	Sécurité	203
7.6	Adresses notoires	204
8	Contrats normatifs	205
8.1	Schéma OPC binaire	205
8.2	Schéma XML et langage WSDL	205
8.3	Schéma du Modèle d'Information	205
8.4	Définition formelle du Modèle d'Information UA	205
8.5	Constantes	205
8.6	Encodage des Types de Données	205
8.7	Configuration de Sécurité	205
Annexe A (normative)	Constantes	206
A.1	Identificateurs d'attributs	206

A.2	Codes de statut.....	206
A.3	Identificateurs de nœud numériques	207
Annexe B (normative)	Nodeset OPC UA	208
Annexe C (normative)	Déclarations de type pour le mapping d'origine OPC UA	209
Annexe D (normative)	Langage WSDL pour le mapping XML	210
D.1	Schéma XML	210
D.2	Types d'accès WDSL	210
D.3	Liaisons WSDL	210
Annexe E (normative)	Gestion des paramètres de sécurité	211
E.1	Vue d'ensemble	211
E.2	SecuredApplication	212
E.3	CertificateIdentifier	216
E.4	CertificateStoreIdentifier	218
E.5	CertificateList.....	218
E.6	CertificateValidationOptions.....	218
Annexe F (normative)	Schéma XML du Modèle d'information	220
F.1	Vue d'ensemble	220
F.2	UANodeSet.....	220
F.3	UANode	222
F.4	Reference	223
F.5	RolePermission.....	223
F.6	UAType.....	223
F.7	UAInstance	224
F.8	UAVariable	224
F.9	UAMethod.....	225
F.10	TranslationType	226
F.11	UADataType	227
F.12	DataTypeDefinition	227
F.13	DataTypeField	228
F.14	Variant.....	229
F.15	Exemple.....	230
F.16	UANodeSetChanges	232
F.17	NodesToAdd	233
F.18	ReferencesToChange	234
F.19	ReferenceToChange	234
F.20	NodesToDelete	234
F.21	NodeToDelete	235
F.22	UANodeSetChangesStatus	235
F.23	NodeSetStatusList	236
F.24	NodeSetStatus.....	236
Bibliographie.....		237
Figure 1 – Vue d'ensemble des piles OPC UA.....		131
Figure 2 – Codage des entiers dans une séquence binaire		137
Figure 3 – Codage des virgules flottantes dans une séquence binaire		138
Figure 4 – Codage des chaînes dans une séquence binaire.....		138
Figure 5 – Codage des Guid dans une séquence binaire.....		139

Figure 6 – Codage d'un Élément Xml dans une séquence binaire	139
Figure 7 – Nodeld de chaîne	141
Figure 8 – Nodeld à deux octets	141
Figure 9 – Nodeld à quatre octets	142
Figure 10 – Protocole d'établissement de liaison de sécurité	174
Figure 11 – MessageChunk de conversation sécurisée OPC UA	182
Figure 12 – Structure d'un Message pour le Protocole de connexion OPC UA	191
Figure 13 – Connexion initiée par le Client via le Protocole de connexion OPC UA	195
Figure 14 – Connexion initiée par le Serveur via le Protocole de connexion OPC UA	195
Figure 15 – Fermeture d'une connexion via le Protocole de connexion OPC UA	196
Figure 16 – Scénarios pour le transport HTTPS	199
Figure 17 – Configuration de la communication via WebSocket.....	203
Tableau 1 – Types de données intégrés.....	133
Tableau 2 – Structure du Guid	133
Tableau 3 – Présentation d'un Décimal	136
Tableau 4 – Types à virgule flottante pris en charge	137
Tableau 5 – Composants de Nodeld	140
Tableau 6 – Valeurs de DataEncoding de Nodeld	140
Tableau 7 – DataEncoding binaire de Nodeld normalisé	140
Tableau 8 – DataEncoding binaire de Nodeld à deux octets.....	141
Tableau 9 – DataEncoding binaire de Nodeld à quatre octets	141
Tableau 10 – DataEncoding binaire d'ExpandedNodeld	142
Tableau 11 – DataEncoding binaire de DiagnosticInfo	143
Tableau 12 – DataEncoding binaire de QualifiedName.....	143
Tableau 13 – DataEncoding binaire de LocalizedText	144
Tableau 14 – DataEncoding binaire d'Objet d'extension	145
Tableau 15 – DataEncoding binaire de Variante.....	146
Tableau 16 – DataEncoding binaire de Valeur de données	147
Tableau 17 – Echantillon de structure à Codage OPC UA binaire	149
Tableau 18 – Echantillon de structure à Codage OPC UA binaire avec champs facultatifs	151
Tableau 19 – Echantillon de structure à Codage OPC UA binaire	152
Tableau 20 – Mappings des types de données XML pour les entiers.....	154
Tableau 21 – Mappings de types de données XML pour les virgules flottantes.....	154
Tableau 22 – Composants de Nodeld	156
Tableau 23 – Composants d'ExpandedNodeld	157
Tableau 24 – Composants d'énumération	161
Tableau 25 – Définition d'Objet JSON pour un Nodeld	166
Tableau 26 – Définition d'Objet JSON pour un ExpandedNodeld	167
Tableau 27 – Définition d'Objet JSON pour un StatusCode	167
Tableau 28 – Définition d'Objet JSON pour une DiagnosticInfo	168
Tableau 29 – Définition d'Objet JSON pour un QualifiedName	168

Tableau 30 – Définition d'objet JSON pour un LocalizedText	169
Tableau 31 – Définition d'Objet JSON pour un ExtensionObject.....	169
Tableau 32 – Définition d'Objet JSON pour une Variante	170
Tableau 33 – Définition d'Objet JSON pour une DataValue	170
Tableau 34 – Définition d'Objet JSON pour un Décimal.....	171
Tableau 35 – Définition d'Objet JSON pour une <i>Structure</i> comportant des champs facultatifs	172
Tableau 36 – Définition d'Objet JSON pour une Union	173
Tableau 37 – SecurityPolicy.....	175
Tableau 38 – Certificat d'instance d'application.....	176
Tableau 39 – UserTokenPolicy Kerberos	178
Tableau 40 – UserTokenPolicy JWT	178
Tableau 41 – Définition d'IssuerEndpointUrl JWT.....	179
Tableau 42 – Revendications de Jeton d'accès	180
Tableau 43 – En-tête de message de conversation OPC UA sécurisée	182
Tableau 44 – En-tête de sécurité d'algorithme asymétrique	183
Tableau 45 – En-tête de sécurité d'algorithme symétrique	184
Tableau 46 – En-tête de séquence.....	184
Tableau 47 – Cartouche de message de conversation OPC UA sécurisée	185
Tableau 48 – Corps de l'abandon de message de conversation OPC UA sécurisée	186
Tableau 49 – Service "OpenSecureChannel" pour une conversation OPC UA sécurisée	187
Tableau 50 – Saisies de PRF pour les SecurityPolicies reposant sur RSA	189
Tableau 51 – Paramètres de génération de clés de cryptographie	189
Tableau 52 – En-tête de Message pour le Protocole de connexion OPC UA	191
Tableau 53 – Message d'accueil pour le Protocole de connexion OPC UA	192
Tableau 54 – Message d'acquiescement pour le Protocole de connexion OPC UA	193
Tableau 55 – Message d'erreur pour le Protocole de connexion OPC UA.....	193
Tableau 56 – Message ReverseHello pour le Protocole de connexion OPC UA.....	194
Tableau 57 – Codes d'erreur pour le Protocole de connexion OPC UA.....	197
Tableau 58 – Mappings de protocoles WebSocket	203
Tableau 59 – Adresses notoires pour les serveurs "Découverte" locaux.....	204
Tableau A.1 – Identificateurs affectés aux attributs	206
Tableau E.1 – SecuredApplication	213
Tableau E.2 – Identificateur de certificat	216
Tableau E.3 – Mémoire de répertoire structurée	217
Tableau E.4 – CertificateStoreIdentifier	218
Tableau E.5 – CertificateList.....	218
Tableau E.6 – CertificateValidationOptions	219
Tableau F.1 – UANodeSet	221
Tableau F.2 – UANode	222
Tableau F.3 – Référence	223
Tableau F.4 – RolePermission	223
Tableau F.5 – Nœuds de type UANodeSet.....	223

Tableau F.6 – Nœuds d'instance UANodeSet	224
Tableau F.7 – UAInstance	224
Tableau F.8 – UVariable	225
Tableau F.9 – UAMethod	225
Tableau F.10 – TranslationType.....	227
Tableau F.11 – UADatatype	227
Tableau F.12 – DataTypeDefinition	228
Tableau F.13 – DataTypeField	229
Tableau F.14 – UANodeSetChanges.....	233
Tableau F.15 – NodesToAdd	233
Tableau F.16 – ReferencesToChange.....	234
Tableau F.17 – ReferencesToChange.....	234
Tableau F.18 – NodesToDelete.....	235
Tableau F.19 – ReferencesToChange.....	235
Tableau F.20 – UANodeSetChangesStatus.....	235
Tableau F.21 – NodeSetStatusList.....	236
Tableau F.22 – NodeSetStatus	236

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ARCHITECTURE UNIFIÉE OPC –

Partie 6: Mappings

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62541-6 a été établie par le sous-comité 65E: Les dispositifs et leur intégration dans les systèmes de l'entreprise, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette troisième édition annule et remplace la deuxième édition parue en 2015. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) codages:

- ajout du codage JSON pour PubSub (irréversible);
- ajout du codage JSON pour le Client/Serveur (réversible);
- ajout de la prise en charge des champs facultatifs dans les structures;

- ajout de la prise en charge des Unions;
- b) mappings de transport:
- ajout de la connexion sécurisée WebSocket (WSS);
 - ajout de la prise en charge de la connectivité inversée;
 - ajout de la prise en charge de l'invocation de service sans session dans HTTPS;
- c) transport déconseillé (absence de prise en charge sur la plupart des plateformes):
- SOAP/HTTP avec WS-SecureConversation (tous les codages);
- d) ajout du mapping pour JSON Web Token;
- e) ajout de la prise en charge des Unions pour le Schéma de NodeSet;
- f) ajout d'opérations par lots permettant d'ajouter/de supprimer des nœuds au niveau du Schéma de NodeSet;
- g) ajout de la prise en charge des matrices multidimensionnelles à l'extérieur des Variantes;
- h) ajout d'une représentation binaire pour les types de données Décimaux;
- i) ajout du mapping pour le Cadre d'autorisation OAuth2.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65E/718/FDIS	65E/734/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Dans l'ensemble du présent document et dans les autres parties de l'IEC 62541, certaines conventions de document sont utilisées:

Le format *italique* est utilisé pour mettre en évidence un terme défini ou une définition qui apparaît à l'Article 3 dans l'une des parties de la série.

Le format *italique* est également utilisé pour mettre en évidence le nom d'un paramètre d'entrée ou de sortie de service, ou le nom d'une structure ou d'un élément de structure habituellement défini dans les tableaux.

Par ailleurs, les *termes* et les *noms en italique* sont, à quelques exceptions près, écrits en camel-case (pratique qui consiste à joindre, sans espace, les éléments des mots ou expressions composés, la première lettre de chaque élément étant en majuscule). Par exemple, le terme défini est *AddressSpace* et non Espace d'adressage. Cela permet de mieux comprendre qu'il existe une définition unique pour *AddressSpace*, et non deux définitions distinctes pour Espace et pour Adressage.

Une liste de toutes les parties de la série IEC 62541, publiées sous le titre général *OPC Unified Architecture*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

ARCHITECTURE UNIFIÉE OPC –

Partie 6: Mappings

1 Domaine d'application

La présente partie de l'IEC 62541 spécifie les mappings de l'Architecture unifiée OPC (OPC UA) entre le modèle de sécurité décrit dans l'IEC TR 62541-2, les définitions de services abstraits spécifiées dans l'IEC 62541-4, les structures de données définies dans l'IEC 62541-5 et les protocoles de réseaux physiques qui peuvent être utilisés pour mettre en œuvre la spécification OPC UA.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TR 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts* (disponible en anglais seulement)

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security Model* (disponible en anglais seulement)

IEC 62541-3, *Architecture unifiée OPC – Partie 3: Modèle d'espace d'adressage*

IEC 62541-4, *Architecture unifiée OPC – Partie 4: Services*

IEC 62541-5, *Architecture unifiée OPC – Partie 5: Modèle d'information*

IEC 62541-7, *Architecture unifiée OPC – Partie 7: Profils*

IEC 62541-12, *Architecture unifiée OPC – Partie 12: Services globaux et de découverte*

ISO 8601-1:2019, *Date et heure – Représentations pour l'échange d'information – Partie 1: Règles de base*

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

SOAP Partie 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* (disponible en anglais seulement)

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)* (disponible en anglais seulement)

IEEE-754: Standard for 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>

PKCS #12: PKCS #12: Personal Information Exchange Syntax
<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>