

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 IEC, Geneva, Switzerland

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

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

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 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 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: csc@iec.ch.

A propos de l'IEC

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

A propos des publications IEC

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

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

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

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

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

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100

ISBN 978-2-8322-2373-4

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

CONTENTS

FOREWORD.....	7
1 Scope.....	9
2 Normative references	9
3 Terms, definitions, abbreviations and symbols.....	11
3.1 Terms and definitions.....	11
3.2 Abbreviations and symbols	11
4 Overview	12
5 Data encoding.....	13
5.1 General.....	13
5.1.1 Overview	13
5.1.2 Built-in Types.....	13
5.1.3 Guid.....	14
5.1.4 ByteString.....	15
5.1.5 ExtensionObject	15
5.1.6 Variant.....	15
5.2 OPC UA Binary	16
5.2.1 General.....	16
5.2.2 Built-in Types.....	16
5.2.3 Enumerations.....	25
5.2.4 Arrays.....	25
5.2.5 Structures	25
5.2.6 Messages	26
5.3 XML	26
5.3.1 Built-in Types.....	26
5.3.2 Enumerations.....	33
5.3.3 Arrays.....	33
5.3.4 Structures	33
5.3.5 Messages	34
6 Message Security Protocols	34
6.1 Security handshake	34
6.2 Certificates	35
6.2.1 General.....	35
6.2.2 Application Instance Certificate.....	36
6.2.3 Signed Software Certificate.....	36
6.3 Time synchronization	37
6.4 UTC and International Atomic Time (TAI).....	37
6.5 Issued User Identity Tokens – Kerberos.....	38
6.6 WS Secure Conversation	38
6.6.1 Overview	38
6.6.2 Notation.....	40
6.6.3 Request Security Token (RST/SCT).....	40
6.6.4 Request Security Token Response (RSTR/SCT).....	41
6.6.5 Using the SCT	42
6.6.6 Cancelling Security contexts	42
6.7 OPC UA Secure Conversation	43
6.7.1 Overview	43

6.7.2	MessageChunk structure	43
6.7.3	MessageChunks and error handling	46
6.7.4	Establishing a SecureChannel	47
6.7.5	Deriving keys	48
6.7.6	Verifying Message Security	49
7	Transport Protocols	50
7.1	OPC UA TCP	50
7.1.1	Overview	50
7.1.2	Message structure	50
7.1.3	Establishing a connection	52
7.1.4	Closing a connection	53
7.1.5	Error handling	54
7.1.6	Error recovery	54
7.2	SOAP/HTTP	56
7.2.1	Overview	56
7.2.2	XML Encoding	56
7.2.3	OPC UA Binary Encoding	57
7.3	HTTPS	57
7.3.1	Overview	57
7.3.2	XML Encoding	59
7.3.3	OPC UA Binary Encoding	60
7.4	Well known addresses	60
8	Normative Contracts	61
8.1	OPC Binary Schema	61
8.2	XML Schema and WSDL	61
Annex A (normative)	Constants	62
A.1	Attribute Ids	62
A.2	Status Codes	62
A.3	Numeric Node Ids	62
Annex B (normative)	OPC UA Nodeset	64
Annex C (normative)	Type declarations for the OPC UA native Mapping	65
Annex D (normative)	WSDL for the XML Mapping	66
D.1	XML Schema	66
D.2	WSDL Port Types	66
D.3	WSDL Bindings	66
Annex E (normative)	Security settings management	67
E.1	Overview	67
E.2	SecuredApplication	68
E.3	CertificateIdentifier	71
E.4	CertificateStoreIdentifier	73
E.5	CertificateList	73
E.6	CertificateValidationOptions	73
Annex F (normative)	Information Model XML Schema	75
F.1	Overview	75
F.2	UANodeSet	75
F.3	UANode	76
F.4	Reference	76
F.5	UAType	77

F.6	UAInstance	77
F.7	UAVariable	77
F.8	UAMethod	78
F.9	TranslationType	78
F.10	UADatatype	79
F.11	DataTypeDefinition	79
F.12	DataTypeField	80
F.13	Variant	80
F.14	Example (Informative)	81
Figure 1	– The OPC UA Stack Overview	13
Figure 2	– Encoding Integers in a binary stream	16
Figure 3	– Encoding Floating Points in a binary stream	17
Figure 4	– Encoding Strings in a binary stream	17
Figure 5	– Encoding GUIDs in a binary stream	18
Figure 6	– Encoding XmlElements in a binary stream	19
Figure 7	– A String NodeId	20
Figure 8	– A Two Byte NodeId	20
Figure 9	– A Four Byte NodeId	21
Figure 10	– Security handshake	34
Figure 11	– Relevant XML Web Services specifications	39
Figure 12	– The WS Secure Conversation handshake	39
Figure 13	– OPC UA Secure Conversation MessageChunk	43
Figure 14	– OPC UA TCP Message structure	52
Figure 15	– Establishing a OPC UA TCP connection	53
Figure 16	– Closing a OPC UA TCP connection	53
Figure 17	– Recovering an OPC UA TCP connection	55
Figure 18	– Scenarios for the HTTPS Transport	58
Table 1	– Built-in Data Types	14
Table 2	– Guid structure	14
Table 3	– Supported Floating Point Types	17
Table 4	– NodeId components	19
Table 5	– NodeId DataEncoding values	19
Table 6	– Standard NodeId Binary DataEncoding	19
Table 7	– Two Byte NodeId Binary DataEncoding	20
Table 8	– Four Byte NodeId Binary DataEncoding	20
Table 9	– ExpandedNodeId Binary DataEncoding	21
Table 10	– DiagnosticInfo Binary DataEncoding	22
Table 11	– QualifiedName Binary DataEncoding	22
Table 12	– LocalizedText Binary DataEncoding	22
Table 13	– Extension Object Binary DataEncoding	23
Table 14	– Variant Binary DataEncoding	24
Table 15	– Data Value Binary DataEncoding	25

Table 16 – Sample OPC UA Binary Encoded structure.....	26
Table 17 – XML Data Type Mappings for Integers.....	27
Table 18 – XML Data Type Mappings for Floating Points	27
Table 19 – Components of NodeId	29
Table 20 – Components of ExpandedNodeId	30
Table 21 – Components of Enumeration	33
Table 22 – SecurityPolicy	35
Table 23 – ApplicationInstanceCertificate	36
Table 24 – SignedSoftwareCertificate	37
Table 25 – Kerberos UserTokenPolicy	38
Table 26 – WS-* Namespace prefixes.....	40
Table 27 – RST/SCT Mapping to an OpenSecureChannel Request.....	41
Table 28 – RSTR/SCT Mapping to an OpenSecureChannel Response.....	42
Table 29 – OPC UA Secure Conversation Message header	44
Table 30 – Asymmetric algorithm Security header.....	44
Table 31 – Symmetric algorithm Security header	45
Table 32 – Sequence header	45
Table 33 – OPC UA Secure Conversation Message footer.....	46
Table 34 – OPC UA Secure Conversation Message abort body.....	47
Table 35 – OPC UA Secure Conversation OpenSecureChannel Service	47
Table 36 – Cryptography key generation parameters	49
Table 37 – OPC UA TCP Message header.....	50
Table 38 – OPC UA TCP Hello Message.....	51
Table 39 – OPC UA TCP Acknowledge Message	51
Table 40 – OPC UA TCP Error Message.....	52
Table 41 – OPC UA TCP error codes	54
Table 42 – WS-Addressing headers	56
Table 43 – Well known addresses for Local Discovery Servers	60
Table A.1 – Identifiers assigned to Attributes	62
Table E.1 – SecuredApplication	69
Table E.2 – CertificateIdentifier.....	71
Table E.3 – Structured directory store.....	72
Table E.4 – CertificateStoreIdentifier	73
Table E.5 – CertificateList.....	73
Table E.6 – CertificateValidationOptions	74
Table F.1 – UANodeSet	75
Table F.2 – UANode	76
Table F.3 – Reference	77
Table F.4 – UANodeSet Type Nodes.....	77
Table F.5 – UANodeSet Instance Nodes	77
Table F.6 – UAInstance	77
Table F.7 – UAVariable.....	78
Table F.8 – UAMethod	78

Table F.9 – TranslationType	79
Table F.10 – UADDataType.....	79
Table F.11 – DataTypeDefinition.....	80
Table F.12 – DataTypeField.....	80

This document is a preview generated by EVS

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 second edition cancels and replaces the first edition published in 2011. This edition constitutes a technical revision.

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

- a) Some applications need to operation in environments with no access to cryptography libraries. To support this a new HTTPS transport has been defined in 7.3;
- b) The padding byte is not long enough to handle asymmetric key sizes larger than 2048 bits. Added an additional padding byte to 6.7.2 to handle this case.
- c) Fixed errors in SOAP action URIs defined in 7.2.2;

- d) Needed a standard way to serialize nodes in an address space. Added the UANodeSet schema defined in Annex F;

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

CDV	Report on voting
65E/377/CDV	65E/405/RVC

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

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

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 publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

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.

generated by EVS

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 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*

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/xmldsig-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>

X690: 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>

3 Terms, definitions, abbreviations and symbols

3.1 Terms and definitions

For the purposes of this document the terms and definitions given in IEC TR 62541-1, IEC TR 62541-2 and IEC 62541-3 as well as the following apply.

3.1.1

DataEncoding

a way to serialize OPC UA Messages and data structures

3.1.2

Mapping

specifies how to implement an OPC UA feature with a specific technology

Note 1 to entry: For example, the OPC UA Binary Encoding is a *Mapping* that specifies how to serialize OPC UA data structures as sequences of bytes.

3.1.3

Security Protocol

ensures the integrity and privacy of UA Messages that are exchanged between OPC UA applications

3.1.4

Stack Profile

a combination of *DataEncodings*, *SecurityProtocol* and *TransportProtocol Mappings*

Note 1 to entry: OPC UA applications implement one or more *StackProfiles* and can only communicate with OPC UA applications that support a *StackProfile* that they support.

3.1.5

Transport Protocol

a way to exchange serialized OPC UA Messages between OPC UA applications

3.2 Abbreviations and symbols

API	Application Programming Interface
ASN.1	Abstract Syntax Notation #1 (used in X690)
BP	WS-I Basic Profile Version
BSP	WS-I Basic Security Profile
CSV	Comma Separated Value (File Format)
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IPSec	Internet Protocol Security
RST	Request Security Token
OID	Object Identifier (used with ASN.1)
RSTR	Request Security Token Response