

OPC unified architecture - Part 6: Mappings

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 62541-6:2015 sisaldab Euroopa standardi EN 62541-6:2015 ingliskeelset teksti.	This Estonian standard EVS-EN 62541-6:2015 consists of the English text of the European standard EN 62541-6:2015.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 29.05.2015.	Date of Availability of the European standard is 29.05.2015.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 25.040.40, 35.100

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:

Aru 10, 10317 Tallinn, Eesti; koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Aru 10, 10317 Tallinn, Estonia; homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English Version

**OPC unified architecture - Part 6: Mappings
(IEC 62541-6:2015)**

Architecture unifiée OPC - Partie 6: Correspondances
(IEC 62541-6:2015)

OPC Unified Architecture - Teil 6: Protokollabbildungen
(IEC 62541-6:2015)

This European Standard was approved by CENELEC on 2015-04-29. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 65E/377/CDV, future edition 2 of IEC 62541-6, prepared by SC 65E "Devices and integration in enterprise systems", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62541-6:2015.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2016-01-29
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2018-04-29

This document supersedes EN 62541-6:2011.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

Endorsement notice

The text of the International Standard IEC 62541-6:2015 was approved by CENELEC as a European Standard without any modification.

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TR 62541-1	-	OPC unified architecture - Part 1: Overview and concepts	CLC/TR 62541-1	-
IEC/TR 62541-2	-	OPC unified architecture - Part 2: Security model	CLC/TR 62541-2	-
IEC 62541-3	-	OPC unified architecture - Part 3: Address Space Model	EN 62541-3	-
IEC 62541-4	-	OPC Unified Architecture - Part 4: Services	EN 62541-4	-
IEC 62541-5	-	OPC unified architecture - Part 5: Information Model	EN 62541-5	-
IEC 62541-7	-	OPC unified architecture - Part 7: Profiles	EN 62541-7	-
IEEE 754	2008	IEEE Standard for Binary Floating-Point Arithmetic	-	-
ITU-T X.509	-	Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	-	-
ITU-T X.690	2002	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-
FIPS PUB 180-2	2002	Secure Hash Standard	-	-
FIPS PUB 197	2001	Advanced Encryption Standard (AES)	-	-
RFC 1305	1992	Network Time Protocol (Version 3) - Specification, Implementation and Analysis	-	-
RFC 2104	1997	HMAC: Keyed-Hashing for Message Authentication	-	-
RFC 2437	1998	PKCS #1: RSA Cryptography Specifications Version 2.0	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
RFC 2616	1999	Hypertext Transfer Protocol - HTTP/1.1	-	-
RFC 3280	2002	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	-	-
RFC 3548	2003	The Base16, Base32, and Base64 Data Encodings	-	-
RFC 3629	2003	UTF-8, a transformation format of ISO 10646	-	-
RFC 4514	2006	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names	-	-
RFC 5246	2008	The Transport Layer Security (TLS) Protocol Version 1.2	-	-
SOAP Part 1	2007	SOAP Version 1.2 - Part 1: Messaging Framework	-	-
SOAP Part 2	2007	SOAP Version 1.2 - Part 2: Adjuncts	-	-
WS-Addressing	2004	Web Services Addressing (WS-Addressing)	-	-
XML Encryption	2002	XML Encryption Syntax and Processing	-	-
XML Schema Part 1	2004	XML Schema - Part 1: Structures	-	-
XML Schema Part 2	2004	XML Schema - Part 2: Datatypes	-	-
XML Signature	2008	XML Signature Syntax and Processing	-	-

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 SecurityProtocols	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

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