
Enotna arhitektura OPC - 12. del: Odkrivanje in globalne storitve (IEC 62541-12:2025)

OPC unified architecture - Part 12: Discovery and global services (IEC 62541-12:2025)

OPC Unified Architecture - Teil 12: Erkundung und globale Dienste (IEC 62541-12:2025)

Architecture unifiée OPC - Partie 12: Services globaux et de découverte (IEC 62541-12:2025)

Ta slovenski standard je istoveten z: EN IEC 62541-12:2026

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

SIST EN IEC 62541-12:2026**en,fr,de**

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN IEC 62541-12

February 2026

ICS 25.040.40

Supersedes EN IEC 62541-12:2020

English Version

**OPC unified architecture - Part 12: Discovery and global
services
(IEC 62541-12:2025)**

Architecture unifiée OPC - Partie 12: Services globaux et de
découverte
(IEC 62541-12:2025)

OPC Unified Architecture - Teil 12: Erkundung und globale
Dienste
(IEC 62541-12:2025)

This European Standard was approved by CENELEC on 2026-01-26. 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

EN IEC 62541-12:2026 (E)

European foreword

The text of document 65E/1051/CDV, future edition 2 of IEC 62541-12, 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 IEC 62541-12:2026.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2027-02-28 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2029-02-28 document have to be withdrawn

This document supersedes EN IEC 62541-12:2020 and all of its amendments and corrigenda (if any).

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

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Sample Document

Endorsement notice

The text of the International Standard IEC 62541-12:2025 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 are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where 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.cencenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62541-1	-	OPC Unified Architecture - Part 1: Overview and concepts	EN IEC 62541-1	-
IEC 62541-2	-	OPC unified architecture - Part 2: Security model	EN IEC 62541-2 ¹	-
IEC 62541-3	-	OPC Unified Architecture - Part 3: Address Space Model	EN IEC 62541-3	-
IEC 62541-4	-	OPC unified architecture - Part 4: Services	EN IEC 62541-4	-
IEC 62541-5	-	OPC Unified architecture - Part 5: Information Model	EN IEC 62541-5	-
IEC 62541-6	-	OPC unified architecture - Part 6: Mappings	EN IEC 62541-6	-
IEC 62541-7	-	OPC Unified Architecture - Part 7: Profiles	EN IEC 62541-7	-
IEC 62541-9	-	OPC Unified Architecture - Part 9: Alarms and Conditions	EN IEC 62541-9	-
IEC 62541-14	-	OPC unified architecture - Part 14: PubSub	EN IEC 62541-14	-
IEC 62541-17	-	OPC unified architecture - Part 17: Alias Names	EN IEC 62541-17	-
IEC 62541-20	-	OPC unified architecture - Part 20: File transfer	EN IEC 62541-20	-
IEC 62541-21	-	OPC Unified architecture - Part 21: Device Onboarding	EN IEC 62541-21	-
ITU-T Recommendation X.500 ISO/IEC 9594-1	-	Information technology - Open Systems interconnection - The Directory: Overview of concepts, models and services	-	-
IETF RFC 2986	-	PKCS #10: Certification Request Syntax Specification Version 1.7	-	-

¹ Under preparation. Stage at the time of publication: FprEN IEC 62541-2:2025.

EN IEC 62541-12:2026 (E)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IETF RFC 5958	-	Asymmetric Key Packages	-	-
IETF RFC 6763	-	DNS-Based Service Discovery	-	-
IETF RFC 7292	-	PKCS #12: Personal Information Exchange Syntax	-	-

Sample Document

get full document from standards.iteh.ai



IEC 62541-12

Edition 2.0 2025-12

INTERNATIONAL STANDARD

**OPC unified architecture -
Part 12: Discovery and global services**

Sample Document

get full document from standards.iteh.ai

CONTENTS

FOREWORD	9
1 Scope	11
2 Normative references	11
3 Terms, definitions and conventions	12
3.1 Terms and definitions	12
3.2 Abbreviations and symbols	14
4 The Discovery Process	15
4.1 Overview	15
4.2 Registration and Announcement of Applications	15
4.2.1 Overview	15
4.2.2 Hosts with a LocalDiscoveryServer	15
4.2.3 Hosts without a LocalDiscoveryServer	16
4.3 The discovery process for Clients to find Servers	16
4.3.1 Overview	16
4.3.2 Simple Discovery with a DiscoveryUrl	17
4.3.3 Local Discovery	17
4.3.4 MulticastSubnet Discovery	18
4.3.5 Global Discovery	19
4.3.6 Combined Discovery Process for Clients	19
4.4 The Discovery Process for Reverse Connections	20
4.4.1 Overview	20
4.4.2 Out-of-band Discovery	20
4.4.3 Global Discovery for Reverse Connections	21
5 Local Discovery Server	21
5.1 Overview	21
5.2 Security Considerations for Multicast DNS	22
5.3 Network Architectures	22
5.3.1 Overview	22
5.3.2 Single MulticastSubnet	22
5.3.3 Multiple MulticastSubnet	23
5.3.4 No MulticastSubnet	23
5.3.5 Domain names and MulticastSubnets	24
6 Global Discovery Server	25
6.1 Overview	25
6.2 Roles and privileges	25
6.3 Client connections to global services	25
6.4 Local Discovery	26
6.5 Application registration workflow	27
6.6 Information Model	29
6.6.1 Overview	29
6.6.2 Directory	30
6.6.3 DirectoryType	30
6.6.4 FindApplications	32
6.6.5 ApplicationRecordDataType	32
6.6.6 RegisterApplication	33
6.6.7 UpdateApplication	34

IEC 62541-12:2025 © IEC 2025

6.6.8	UnregisterApplication	35
6.6.9	GetApplication	36
6.6.10	QueryApplications	37
6.6.11	QueryServers (deprecated).....	39
6.6.12	ApplicationRegistrationChangedAuditEventType.....	41
7	Certificate Management.....	41
7.1	Overview	41
7.2	Roles and Privileges	42
7.3	Pull Management	43
7.4	Push Management	44
7.5	Application Setup.....	45
7.6	Pull Management workflow	45
7.7	Push Management workflow.....	48
7.8	Common Information Model	50
7.8.1	Overview	50
7.8.2	TrustLists	50
7.8.3	CertificateGroups	60
7.8.4	CertificateTypes	63
7.9	Information Model for Pull Certificate Management	68
7.9.1	Overview	68
7.9.2	CertificateDirectoryType	68
7.9.3	StartSigningRequest.....	70
7.9.4	StartNewKeyPairRequest	72
7.9.5	FinishRequest	74
7.9.6	RevokeCertificate	75
7.9.7	GetCertificateGroups	76
7.9.8	GetCertificates	77
7.9.9	GetTrustList.....	78
7.9.10	GetCertificateStatus	79
7.9.11	CheckRevocationStatus.....	80
7.9.12	CertificateRequestedAuditEventType.....	81
7.9.13	CertificateDeliveredAuditEventType.....	81
7.10	Information Model for Push Certificate Management	82
7.10.1	Overview	82
7.10.2	ServerConfiguration.....	84
7.10.3	ServerConfigurationType	84
7.10.4	UpdateCertificate.....	86
7.10.5	GetCertificates	88
7.10.6	ApplyChanges	88
7.10.7	CreateSigningRequest.....	89
7.10.8	CancelChanges	91
7.10.9	GetRejectedList.....	91
7.10.10	ResetToServerDefaults.....	92
7.10.11	TransactionDiagnosticsType.....	93
7.10.12	TransactionErrorType	94
7.10.13	CertificateUpdateRequestedAuditEventType.....	94
7.10.14	CertificateUpdatedAuditEventType	95
8	KeyCredential Management.....	95
8.1	Overview	95

8.2	Roles and Privileges	96
8.3	Pull Management	96
8.4	Push Management	97
8.5	Information Model for Pull Management	98
8.5.1	Overview	98
8.5.2	KeyCredentialManagementFolderType	99
8.5.3	KeyCredentialManagement	99
8.5.4	KeyCredentialServiceType	99
8.5.5	StartRequest	100
8.5.6	FinishRequest	102
8.5.7	Revoke	103
8.5.8	KeyCredentialAuditEventType	104
8.5.9	KeyCredentialRequestedAuditEventType	104
8.5.10	KeyCredentialDeliveredAuditEventType	105
8.5.11	KeyCredentialRevokedAuditEventType	105
8.6	Information Model for Push Management	106
8.6.1	General	106
8.6.2	KeyCredentialConfigurationFolderType	106
8.6.3	CreateCredential	107
8.6.4	KeyCredentialConfiguration	108
8.6.5	KeyCredentialConfigurationType	108
8.6.6	GetEncryptingKey	109
8.6.7	UpdateCredential	110
8.6.8	DeleteCredential	111
8.6.9	KeyCredentialUpdatedAuditEventType	111
8.6.10	KeyCredentialDeletedAuditEventType	112
9	AuthorizationServices	112
9.1	Overview	112
9.2	Roles and Privileges	113
9.3	Implicit	113
9.4	Explicit	114
9.5	Chained	115
9.6	Information model for requesting Access Tokens	116
9.6.1	Overview	116
9.6.2	AuthorizationServicesFolderType	117
9.6.3	AuthorizationServices	117
9.6.4	AuthorizationServiceType	118
9.6.5	RequestAccessToken	118
9.6.6	GetServiceDescription	120
9.6.7	AccessTokenIssuedAuditEventType	120
9.7	Information Model for Configuring Servers	121
9.7.1	Overview	121
9.7.2	AuthorizationServiceConfigurationFolderType	121
9.7.3	AuthorizationServices	122
9.7.4	AuthorizationServiceConfigurationType	122
10	Namespaces	123
10.1	Namespace Metadata	123
10.2	Handling of OPC UA Namespaces	123
Annex A (informative)	Deployment and configuration	125

IEC 62541-12:2025 © IEC 2025

A.1	Firewalls and discovery.....	125
A.2	Resolving References to Remote Servers.....	127
Annex B	(normative) NodeSet and Constants.....	129
B.1	NodeSet.....	129
B.2	Numeric Node Ids.....	129
Annex C	(normative) OPC UA Mapping to mDNS.....	130
C.1	DNS Server (SRV) record cyntax.....	130
C.2	DNS Text (TXT) record syntax.....	130
C.3	DiscoveryUrl mapping.....	131
Annex D	(normative) Server Capability Identifiers.....	132
Annex E	(normative) DirectoryServices.....	133
E.1	Global Discovery via Other Directory Services.....	133
E.2	UDDI.....	133
E.3	LDAP.....	134
Annex F	(normative) Local Discovery Server.....	136
F.1	Certificate Store Directory Layout.....	136
F.2	Installation Directories on Windows.....	137
Annex G	(normative) Application Setup.....	138
G.1	Application Setup with Pull Management.....	138
G.2	Application Setup with the Push Management.....	138
G.3	Setting Permissions.....	139
Annex H	(informative) Comparison with RFC 7030.....	140
H.1	Overview.....	140
H.2	Obtaining CA Certificates.....	140
H.3	Initial Enrolment.....	140
H.4	Client Certificate Reissuance.....	141
H.5	Server Key Generation.....	141
H.6	Certificate Signing Request (CSR) Attributes Request.....	141
Bibliography	142
Figure 1	– The Registration Process with an LDS.....	16
Figure 2	– The Simple Discovery Process.....	17
Figure 3	– The Local Discovery Process.....	18
Figure 4	– The MulticastSubnet Discovery Process.....	18
Figure 5	– The Global Discovery Process.....	19
Figure 6	– The Discovery Process for Clients.....	20
Figure 7	– The Global Discovery Process for Reverse Connections.....	21
Figure 8	– The Single MulticastSubnet Architecture.....	22
Figure 9	– The Multiple MulticastSubnet Architecture.....	23
Figure 10	– The No MulticastSubnet Architecture.....	24
Figure 11	– The Relationship between GDS and other components.....	26
Figure 12	– Application Registration Workflow.....	28
Figure 13	– The Address Space for the GDS.....	30
Figure 14	– The Pull Management Model for Certificates.....	43
Figure 15	– The Push Certificate Management Model.....	44
Figure 16	– Certificate Pull Management workflow.....	46

Figure 17 – The Pull Management Private Key options	47
Figure 18 – The Certificate Push Management workflow	49
Figure 19 – The Push Management Private Key options	50
Figure 20 – The Certificate Management AddressSpace for the GlobalDiscoveryServer	68
Figure 21 – The AddressSpace for the Server that supports Push Management.....	82
Figure 22 – The Transaction Lifecycle when using PushManagement	83
Figure 23 – The Pull Model for KeyCredential Management	97
Figure 24 – The Push Model for KeyCredential Management	98
Figure 25 – The Address Space used for Pull KeyCredential Management.....	98
Figure 26 – The Address Space used for Push KeyCredential Management.....	106
Figure 27 – Roles and AuthorizationServices	113
Figure 28 – Implicit Authorization	114
Figure 29 – Explicit Authorization.....	115
Figure 30 – Chained Authorization	116
Figure 31 – The Model for Requesting Access Tokens from AuthorizationServices	117
Figure 32 – The Model for Configuring Servers to use AuthorizationServices.....	121
Figure A.1 – Discovering Servers outside a firewall	125
Figure A.2 – Discovering Servers behind a firewall	126
Figure A.3 – Using a Discovery Server with a firewall	127
Figure A.4 – Following References to remote Servers.....	128
Figure E.1 – The UDDI or LDAP Discovery Process.....	133
Figure E.2 – UDDI Registry Structure	134
Figure E.3 – Sample LDAP Hierarchy	135
Table 1 – Well-known Roles for a GDS	25
Table 2 – Privileges for a GDS.....	25
Table 3 – Application Registration Workflow Steps	29
Table 4 – Directory Object Definition.....	30
Table 5 – DirectoryType Definition	31
Table 6 – FindApplications Method AddressSpace Definition	32
Table 7 – ApplicationRecordDataType Structure	33
Table 8 – ApplicationRecordDataType Definition	33
Table 9 – RegisterApplication Method AddressSpace Definition.....	34
Table 10 – UpdateApplication Method AddressSpace Definition.....	35
Table 11 – UnregisterApplication Method AddressSpace Definition.....	36
Table 12 – GetApplication Method AddressSpace Definition	36
Table 13 – ApplicationRecordDataType to ApplicationDescription Mapping.....	37
Table 14 – QueryApplications Method AddressSpace Definition.....	39
Table 15 – ApplicationRecordDataType to ServerOnNetwork Mapping.....	39
Table 16 – QueryServers Method AddressSpace Definition	41
Table 17 – ApplicationRegistrationChangedAuditEventType Definition.....	41
Table 18 – Well-known Roles for a CertificateManager	42
Table 19 – Well-known Roles for Server managed by a CertificateManager	42

Table 20 – Privileges for a CertificateManager.....	43
Table 21 – Certificate Pull Management workflow steps.....	47
Table 22 – TrustListType Definition.....	51
Table 23 – OpenWithMasks Method AddressSpace Definition.....	52
Table 24 – CloseAndUpdate Method AddressSpace Definition.....	54
Table 25 – AddCertificate Method AddressSpace Definition.....	55
Table 26 – RemoveCertificate Method AddressSpace Definition.....	56
Table 27 – TrustListDataType Structure.....	56
Table 28 – TrustListDataType Definition.....	56
Table 29 – TrustListMasks Enumeration.....	57
Table 30 – TrustListMasks Definition.....	57
Table 31 – TrustListValidationOptions Values.....	57
Table 32 – TrustListValidationOptions Definition.....	58
Table 33 – TrustListOutOfDateAlarmType definition.....	58
Table 34 – TrustListUpdateRequestedAuditEventType Definition.....	59
Table 35 – TrustListUpdatedAuditEventType Definition.....	59
Table 36 – CertificateGroupType Definition.....	60
Table 37 – GetRejectedList Method AddressSpace Definition.....	62
Table 38 – CertificateGroupFolderType Definition.....	62
Table 39 – CertificateType Definition.....	63
Table 40 – ApplicationCertificateType Definition.....	63
Table 41 – HttpsCertificateType Definition.....	64
Table 42 – RsaMinApplicationCertificateType Definition.....	64
Table 43 – RsaSha256ApplicationCertificateType Definition.....	65
Table 44 – EccApplicationCertificateType Definition.....	65
Table 45 – EccNistP256ApplicationCertificateType Definition.....	65
Table 46 – EccNistP384ApplicationCertificateType Definition.....	66
Table 47 – EccBrainpoolP256r1ApplicationCertificateType Definition.....	66
Table 48 – EccBrainpoolP384r1ApplicationCertificateType Definition.....	67
Table 49 – EccCurve25519ApplicationCertificateType Definition.....	67
Table 50 – EccCurve448ApplicationCertificateType Definition.....	67
Table 51 – CertificateDirectoryType ObjectType Definition.....	69
Table 52 – StartSigningRequest Method AddressSpace Definition.....	72
Table 53 – StartNewKeyPairRequest Method AddressSpace Definition.....	74
Table 54 – FinishRequest Method AddressSpace Definition.....	75
Table 55 – Revoke Method AddressSpace Definition.....	76
Table 56 – GetCertificateGroups Method AddressSpace Definition.....	77
Table 57 – GetCertificates Method AddressSpace Definition.....	78
Table 58 – GetTrustList Method AddressSpace Definition.....	79
Table 59 – GetCertificateStatus Method AddressSpace Definition.....	80
Table 60 – CheckRevocationStatus Method AddressSpace Definition.....	81
Table 61 – CertificateRequestedAuditEventType Definition.....	81
Table 62 – CertificateDeliveredAuditEventType Definition.....	82

Table 63 – ServerConfiguration Object Definition	84
Table 64 – ServerConfigurationType Definition	85
Table 65 – UpdateCertificate Method AddressSpace Definition	87
Table 66 – GetCertificates Method AddressSpace Definition	88
Table 67 – ApplyChanges Method AddressSpace Definition	89
Table 68 – CreateSigningRequest Method AddressSpace Definition	90
Table 69 – CancelChanges Method AddressSpace Definition	91
Table 70 – GetRejectedList Method AddressSpace Definition	92
Table 71 – ResetToServerDefaults Method AddressSpace Definition	93
Table 72 – TransactionDiagnosticsType Definition	93
Table 73 – TransactionErrorType Structure	94
Table 74 – TransactionErrorType Definition	94
Table 75 – CertificateUpdateRequestedAuditEventType Definition	94
Table 76 – CertificateUpdatedAuditEventType Definition	95
Table 77 – Well-known Roles for a KeyCredentialService	96
Table 78 – Well-known Roles for Server managed by a KeyCredentialService	96
Table 79 – Privileges for a KeyCredentialService	96
Table 80 – KeyCredentialManagementFolderType Definition	99
Table 81 – KeyCredentialManagement Object Definition	99
Table 82 – KeyCredentialServiceType Definition	100
Table 83 – StartRequest Method AddressSpace Definition	102
Table 84 – FinishRequest Method AddressSpace Definition	103
Table 85 – Revoke Method AddressSpace Definition	104
Table 86 – KeyCredentialAuditEventType Definition	104
Table 87 – KeyCredentialRequestedAuditEventType Definition	105
Table 88 – KeyCredentialDeliveredAuditEventType Definition	105
Table 89 – KeyCredentialRevokedAuditEventType Definition	106
Table 90 – KeyCredentialConfigurationFolderType Definition	107
Table 91 – CreateCredential Method AddressSpace Definition	108
Table 92 – KeyCredentialConfiguration Object Definition	108
Table 93 – KeyCredentialConfigurationType Definition	108
Table 94 – GetEncryptingKey Method AddressSpace Definition	110
Table 95 – UpdateCredential Method AddressSpace Definition	111
Table 96 – DeleteCredential Method AddressSpace Definition	111
Table 97 – KeyCredentialUpdatedAuditEventType Definition	112
Table 98 – KeyCredentialDeletedAuditEventType Definition	112
Table 99 – Well-known Roles for an AuthorizationService	113
Table 100 – Privileges for an AuthorizationService	113
Table 101 – AuthorizationServicesFolderType Definition	117
Table 102 – AuthorizationServices Object Definition	117
Table 103 – AuthorizationServiceType Definition	118
Table 104 – RequestAccessToken Method AddressSpace Definition	119
Table 105 – GetServiceDescription Method AddressSpace Definition	120

Table 106 – AccessTokenIssuedAuditEventType Definition	121
Table 107 – AuthorizationServicesFolderType Definition.....	122
Table 108 – AuthorizationServices Object Definition	122
Table 109 – AuthorizationServiceConfigurationType Definition	122
Table 110 – NamespaceMetadata Object for this Document	123
Table 111 – Namespaces used in this document.....	124
Table C.1 – Allowed mDNS service names	130
Table C.2 – DNS TXT record string format.....	131
Table C.3 – DiscoveryUrl to DNS SRV and TXT record mapping.....	131
Table D.1 – Examples of CapabilityIdentifiers	132
Table E.1 – UDDI tModels	134
Table E.2 – LDAP Object Class Schema.....	135
Table F.1 – Application Certificate Store Directory Layout	136
Table H.1 – Verifying that a Server is allowed to Provide Certificates	140
Table H.2 – Verifying that a Client is allowed to request Certificates	140

Sample Document

get full document from standards.iteh.ai