



IEC 62541-12

Edition 1.0 2020-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

**Architecture unifiée OPC –
Partie 12: Services globaux et de découverte**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-8455-1

**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.....	8
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, abbreviated terms and conventions	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms and symbols	13
3.3 Conventions for namespaces	13
4 The discovery process.....	14
4.1 Overview.....	14
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 Security	17
4.3.3 Simple Discovery with a DiscoveryUrl	17
4.3.4 Local Discovery	17
4.3.5 MulticastSubnet Discovery.....	18
4.3.6 Global Discovery	19
4.3.7 Combined Discovery Process for Clients	19
5 Local Discovery Server.....	20
5.1 Overview.....	20
5.2 Security considerations for Multicast DNS.....	21
6 Global Discovery Server	21
6.1 Overview.....	21
6.2 Network architectures	22
6.2.1 Overview	22
6.2.2 Single MulticastSubnet	22
6.2.3 Multiple MulticastSubnet.....	23
6.2.4 No MulticastSubnet.....	23
6.2.5 Domain Names and MulticastSubnets.....	24
6.3 Information Model	25
6.3.1 Overview	25
6.3.2 Directory.....	25
6.3.3 DirectoryType	25
6.3.4 FindApplications	26
6.3.5 ApplicationRecordDataType.....	27
6.3.6 RegisterApplication.....	28
6.3.7 UpdateApplication	29
6.3.8 UnregisterApplication	30
6.3.9 GetApplication	30
6.3.10 QueryApplications	31
6.3.11 QueryServers (deprecated).....	33
6.3.12 ApplicationRegistrationChangedAuditEventType.....	34
7 Certificate management overview	35

7.1	Overview.....	35
7.2	Pull Management.....	36
7.3	Push management.....	36
7.4	Provisioning.....	37
7.5	Common Information Model.....	38
7.5.1	Overview.....	38
7.5.2	TrustListType.....	38
7.5.3	OpenWithMasks.....	39
7.5.4	CloseAndUpdate.....	40
7.5.5	AddCertificate.....	41
7.5.6	RemoveCertificate.....	42
7.5.7	TrustListDataType.....	42
7.5.8	TrustListMasks.....	43
7.5.9	TrustListOutOfDateAlarmType.....	43
7.5.10	CertificateGroupType.....	43
7.5.11	CertificateType.....	44
7.5.12	ApplicationCertificateType.....	45
7.5.13	HttpsCertificateType.....	45
7.5.14	UserCredentialCertificateType.....	45
7.5.15	RsaMinApplicationCertificateType.....	46
7.5.16	RsaSha256ApplicationCertificateType.....	46
7.5.17	CertificateGroupFolderType.....	46
7.5.18	TrustListUpdatedAuditEventType.....	47
7.6	Information Model for Pull Certificate Management.....	48
7.6.1	Overview.....	48
7.6.2	CertificateDirectoryType.....	48
7.6.3	StartSigningRequest.....	49
7.6.4	StartNewKeyPairRequest.....	51
7.6.5	FinishRequest.....	53
7.6.6	GetCertificateGroups.....	54
7.6.7	GetTrustList.....	55
7.6.8	GetCertificateStatus.....	56
7.6.9	CertificateRequestedAuditEventType.....	57
7.6.10	CertificateDeliveredAuditEventType.....	58
7.7	Information Model for Push Certificate Management.....	58
7.7.1	Overview.....	58
7.7.2	ServerConfiguration.....	59
7.7.3	ServerConfigurationType.....	59
7.7.4	UpdateCertificate.....	61
7.7.5	ApplyChanges.....	62
7.7.6	CreateSigningRequest.....	63
7.7.7	GetRejectedList.....	64
7.7.8	CertificateUpdatedAuditEventType.....	64
8	KeyCredential management.....	65
8.1	Overview.....	65
8.2	Pull management.....	66
8.3	Push management.....	66
8.4	Information Model for pull management.....	67
8.4.1	Overview.....	67

8.4.2	KeyCredentialManagement	68
8.4.3	KeyCredentialServiceType	68
8.4.4	StartRequest	69
8.4.5	FinishRequest	70
8.4.6	Revoke	71
8.4.7	KeyCredentialAuditEventType	72
8.4.8	KeyCredentialRequestedAuditEventType	73
8.4.9	KeyCredentialDeliveredAuditEventType	73
8.4.10	KeyCredentialRevokedAuditEventType	73
8.5	Information Model for push management	74
8.5.1	General	74
8.5.2	KeyCredentialConfiguration	74
8.5.3	KeyCredentialConfigurationType	75
8.5.4	UpdateCredential	75
8.5.5	DeleteCredential	76
8.5.6	KeyCredentialUpdatedAuditEventType	77
8.5.7	KeyCredentialDeletedAuditEventType	77
9	Authorization Services	78
9.1	Overview	78
9.2	Implicit	78
9.3	Explicit	79
9.4	Chained	80
9.5	Information Model for Requesting Access Tokens	81
9.5.1	Overview	81
9.5.2	AuthorizationServices	82
9.5.3	AuthorizationServiceType	82
9.5.4	RequestAccessToken	83
9.5.5	GetServiceDescription	84
9.5.6	AccessTokenIssuedAuditEventType	85
9.6	Information Model for configuring Servers	85
9.6.1	Overview	85
9.6.2	AuthorizationServices	86
9.6.3	AuthorizationServiceConfigurationType	86
Annex A (informative)	Deployment and configuration	87
A.1	Firewalls and discovery	87
A.2	Resolving references to remote Servers	89
Annex B (normative)	Constants	91
Annex C (normative)	OPC UA Mapping to mDNS	92
C.1	DNS Server (SRV) record syntax	92
C.2	DNS Text (TXT) record syntax	92
C.3	DiscoveryUrl mapping	93
Annex D (normative)	Server Capability Identifiers	94
Annex E (normative)	DirectoryServices	95
E.1	Global Discovery via other directory services	95
E.2	UDDI	95
E.3	LDAP	96
Annex F (normative)	Local Discovery Server	98
F.1	Certificate store directory layout	98

F.2	Installation directories on Windows	99
Annex G (normative)	Application installation process	100
G.1	Provisioning with Pull Management	100
G.2	Provisioning with Push Management	100
G.3	Setting permissions	101
Annex H (informative)	Comparison with RFC 7030	102
H.1	Overview	102
H.2	Obtaining CA Certificates	102
H.3	Initial enrolment	102
H.4	Client Certificate reissuance	103
H.5	Server key generation	103
H.6	Certificate Signing Request (CSR) attributes request	103
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 relationship between GDS and other components	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 Address Space for the GDS	25
Figure 12	– The Pull Certificate management model	36
Figure 13	– The Push Certificate management model	37
Figure 14	– The Certificate Management AddressSpace for the GlobalDiscoveryServer	48
Figure 15	– The AddressSpace for the Server that supports Push Management	59
Figure 16	– The Pull Model for KeyCredential management	66
Figure 17	– The Push Model for KeyCredential management	67
Figure 18	– The Address Space used for Pull KeyCredential management	68
Figure 19	– The AddressSpace used for Push KeyCredential management	74
Figure 20	– Roles and Authorization Services	78
Figure 21	– Implicit authorization	79
Figure 22	– Explicit authorization	80
Figure 23	– Chained authorization	81
Figure 24	– The Model for Requesting Access Tokens from Authorization Services	82
Figure 25	– The Model for configuring Servers to use Authorization Services	85
Figure A.1	– Discovering Servers outside a firewall	87
Figure A.2	– Discovering Servers behind a firewall	88
Figure A.3	– Using a Discovery Server with a firewall	89
Figure A.4	– Following References to Remote Servers	90
Figure E.1	– The UDDI or LDAP Discovery process	95
Figure E.2	– UDDI registry structure	96

Figure E.3 – Sample LDAP hierarchy	97
Table 1 – GDS NamespaceMetadataType Object definition	14
Table 2 – Directory Object definition	25
Table 3 – DirectoryType definition.....	26
Table 4 – FindApplications Method AddressSpace definition.....	27
Table 5 – ApplicationRecordDataType definition	28
Table 6 – RegisterApplication Method AddressSpace definition	29
Table 7 – UpdateApplication Method AddressSpace definition	30
Table 8 – UnregisterApplication Method AddressSpace definition	30
Table 9 – GetApplication Method AddressSpace definition.....	31
Table 10 – QueryApplications Method AddressSpace definition	33
Table 11 – QueryServers Method AddressSpace definition	34
Table 12 – ApplicationRegistrationChangedAuditEventType definition	35
Table 13 – TrustListType definition	39
Table 14 – OpenWithMasks Method AddressSpace definition	40
Table 15 – CloseAndUpdate Method AddressSpace definition	41
Table 16 – AddCertificate Method AddressSpace definition	41
Table 17 – RemoveCertificate Method AddressSpace definition	42
Table 18 – TrustListDataType definition	42
Table 19 – TrustListMasks values	43
Table 20 – TrustListOutOfDateAlarmType definition.....	43
Table 21 – CertificateGroupType definition	44
Table 22 – CertificateType definition	45
Table 23 – ApplicationCertificateType definition.....	45
Table 24 – HttpsCertificateType definition.....	45
Table 25 – UserCredentialCertificateType definition.....	46
Table 26 – RsaMinApplicationCertificateType definition	46
Table 27 – RsaSha256ApplicationCertificateType definition.....	46
Table 28 – CertificateGroupFolderType definition	47
Table 29 – TrustListUpdatedAuditEventType definition	47
Table 30 – CertificateDirectoryType ObjectType definition	49
Table 31 – StartSigningRequest Method AddressSpace definition.....	51
Table 32 – StartNewKeyPairRequest Method AddressSpace definition	53
Table 33 – FinishRequest Method AddressSpace definition	54
Table 34 – GetCertificateGroups Method AddressSpace definition.....	55
Table 35 – GetTrustList Method AddressSpace definition	56
Table 36 – GetCertificateStatus Method AddressSpace definition	57
Table 37 – CertificateRequestedAuditEventType definition	58
Table 38 – CertificateDeliveredAuditEventType definition	58
Table 39 – ServerConfiguration Object definition	59
Table 40 – ServerConfigurationType definition.....	60
Table 41 – UpdateCertificate Method AddressSpace Definition	62

Table 42 – ApplyChanges Method AddressSpace Definition	63
Table 43 – CreateSigningRequest Method AddressSpace definition.....	64
Table 44 – GetRejectedList Method AddressSpace definition.....	64
Table 45 – CertificateUpdatedAuditEventType definition	65
Table 46 – KeyCredentialManagement Object definition	68
Table 47 – KeyCredentialServiceType definition	69
Table 48 – StartRequest Method AddressSpace definition	70
Table 49 – FinishRequest Method AddressSpace definition	71
Table 50 – Revoke Method AddressSpace definition.....	72
Table 51 – KeyCredentialAuditEventType definition	72
Table 52 – KeyCredentialRequestedAuditEventType definition	73
Table 53 – KeyCredentialDeliveredAuditEventType definition	73
Table 54 – KeyCredentialRevokedAuditEventType definition	74
Table 55 – KeyCredentialConfiguration Object definition.....	74
Table 56 – KeyCredentialConfigurationType definition	75
Table 57 – UpdateCredential Method AddressSpace definition	76
Table 58 – DeleteCredential Method AddressSpace definition	77
Table 59 – KeyCredentialUpdatedAuditEventType definition	77
Table 60 – KeyCredentialUpdatedAuditEventType definition	77
Table 61 – AuthorizationServices Object definition.....	82
Table 62 – AuthorizationServiceType definition.....	82
Table 63 – RequestAccessToken Method AddressSpace definition	84
Table 64 – GetServiceDescription Method AddressSpace definition.....	85
Table 65 – AccessTokenIssuedAuditEventType definition	85
Table 66 – AuthorizationServices Object definition.....	86
Table 67 – AuthorizationServiceConfigurationType definition	86
Table C.1 – Allowed mDNS service names	92
Table C.2 – DNS TXT record string format.....	93
Table C.3 – DiscoveryUrl to DNS SRV and TXT Record Mapping	93
Table D.1 – Examples of <i>ServerCapabilityIdentifiers</i>	94
Table E.1 – UDDI tModels.....	96
Table E.2 – LDAP object class schema.....	97
Table F.1 – Application Certificate store directory layout.....	98
Table H.1 – Verifying that a Server is allowed to provide Certificates.....	102
Table H.2 – Verifying that a Client is allowed to request Certificates	102

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 12: Discovery and global services

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 62541-12 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65E/711/FDIS	65E/723/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 the IEC 62541 series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in the "Terms and definition" clause in one of the parts of the IEC 62541 series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms and names* are, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example, the defined term is AddressSpace instead of Address Space. This makes it easier to understand that there is a single definition for AddressSpace, not separate definitions for Address and Space.

A list of all parts 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.

OPC UNIFIED ARCHITECTURE –

Part 12: Discovery and global services

1 Scope

This part of IEC 62541 specifies how OPC Unified Architecture (OPC UA) *Clients* and *Servers* interact with *DiscoveryServers* when used in different scenarios. It specifies the requirements for the *LocalDiscoveryServer*, *LocalDiscoveryServer-ME* and *GlobalDiscoveryServer*. It also defines information models for *Certificate* management, *KeyCredential* management and *Authorization Services*.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 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 62541-6, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-7, *OPC Unified Architecture – Part 7: Profiles*

IEC 62541-9, *OPC Unified Architecture – Part 9: Alarms and conditions*

IEC 62541-14, *OPC Unified Architecture – Part 14: PubSub*

X.500: ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory – Part 1: Overview of concepts, models and services*

IETF RFC 1035, *DNS-Name: Domain Names – Implementation and Specification*
<http://www.ietf.org/rfc/rfc1035.txt>

IETF RFC 2986, *PKCS #10: Certification Request Syntax Specification*
<http://www.ietf.org/rfc/rfc2986.txt>

IETF RFC 3927, *Auto-IP: Dynamic Configuration of IPv4 Link-Local Addresses*
<http://www.ietf.org/rfc/rfc3927.txt>

IETF RFC 5958, *Asymmetric Key Packages*
<http://www.ietf.org/rfc/rfc5958.txt>

IETF RFC 6762, *mDNS: Multicast DNS*
<http://www.ietf.org/rfc/rfc6762.txt>

IETF RFC 6763, *DNS-SD: DNS Based Service Discovery*
<http://www.ietf.org/rfc/rfc6763.txt>

IETF RFC 7030: *Enrollment over Secure Transport*
<http://www.ietf.org/rfc/rfc7030.txt>

PKCS #12: *Personal Information Exchange Syntax*
<http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11301-wp-pkcs-12v1-1-personal-information-exchange-syntax.pdf>

DI: *OPC Unified Architecture for Devices (DI)*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-devices-di/>

ADI: *OPC Unified Architecture for Analyzer Devices (ADI)*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-analyzer-devices-adi/>

PLCopen: *OPC Unified Architecture / PLCopen Information Model*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-plcopen-information-model/>

FDI: *OPC Unified Architecture for FDI*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-fdi/>

ISA-95: *ISA-95 Common Object Model*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/isa-95-common-object-model/>

SOMMAIRE

AVANT-PROPOS	110
1 Domaine d'application	112
2 Références normatives	112
3 Termes, définitions, termes abrégés et conventions	113
3.1 Termes et définitions	113
3.2 Termes abrégés et symboles	115
3.3 Conventions pour les espaces de noms	116
4 Processus de découverte	116
4.1 Vue d'ensemble	116
4.2 Enregistrement et annonce d'Applications	117
4.2.1 Vue d'ensemble	117
4.2.2 Hôtes avec un LocalDiscoveryServer	117
4.2.3 Hôtes sans LocalDiscoveryServer	118
4.3 Processus de découverte permettant aux Clients de trouver des Serveurs	118
4.3.1 Vue d'ensemble	118
4.3.2 Sécurité	119
4.3.3 Découverte simple avec une DiscoveryUrl	119
4.3.4 Découverte locale	119
4.3.5 Découverte de MulticastSubnet	120
4.3.6 Découverte globale	121
4.3.7 Processus de découverte combiné pour les Clients	122
5 Serveur de découverte local	122
5.1 Vue d'ensemble	122
5.2 Considérations relatives à la sécurité pour Multicast DNS	123
6 Serveur de découverte global	123
6.1 Vue d'ensemble	123
6.2 Architectures réseau	124
6.2.1 Vue d'ensemble	124
6.2.2 MulticastSubnet simple	124
6.2.3 MulticastSubnets multiples	125
6.2.4 Sans MulticastSubnet	126
6.2.5 Noms de domaine et MulticastSubnets	126
6.3 Modèle d'Information	127
6.3.1 Vue d'ensemble	127
6.3.2 Répertoire	127
6.3.3 DirectoryType	128
6.3.4 FindApplications	129
6.3.5 ApplicationRecordDataType	129
6.3.6 RegisterApplication	130
6.3.7 UpdateApplication	131
6.3.8 UnregisterApplication	132
6.3.9 GetApplication	132
6.3.10 QueryApplications	133
6.3.11 QueryServers (obsolète)	135
6.3.12 ApplicationRegistrationChangedAuditEventType	136
7 Vue d'ensemble de la gestion des certificats	137

7.1	Vue d'ensemble	137
7.2	Gestion en flux tiré.....	138
7.3	Gestion en flux poussé	139
7.4	Approvisionnement	140
7.5	Modèle d'information commun.....	140
7.5.1	Vue d'ensemble	140
7.5.2	TrustListType.....	140
7.5.3	OpenWithMasks	141
7.5.4	CloseAndUpdate.....	142
7.5.5	AddCertificate.....	143
7.5.6	RemoveCertificate	144
7.5.7	TrustListDataType	145
7.5.8	TrustListMasks	145
7.5.9	TrustListOutOfDateAlarmType	145
7.5.10	CertificateGroupType.....	146
7.5.11	CertificateType	147
7.5.12	ApplicationCertificateType	147
7.5.13	HttpsCertificateType	147
7.5.14	UserCredentialCertificateType	147
7.5.15	RsaMinApplicationCertificateType	148
7.5.16	RsaSha256ApplicationCertificateType	148
7.5.17	CertificateGroupFolderType.....	148
7.5.18	TrustListUpdatedAuditEventType.....	149
7.6	Modèle d'information pour la gestion des certificats en flux tiré.....	150
7.6.1	Vue d'ensemble	150
7.6.2	CertificateDirectoryType	150
7.6.3	StartSigningRequest.....	152
7.6.4	StartNewKeyPairRequest	153
7.6.5	FinishRequest	155
7.6.6	GetCertificateGroups	156
7.6.7	GetTrustList.....	157
7.6.8	GetCertificateStatus	158
7.6.9	CertificateRequestedAuditEventType.....	159
7.6.10	CertificateDeliveredAuditEventType.....	160
7.7	Modèle d'information pour la gestion des certificats en flux poussé.....	160
7.7.1	Vue d'ensemble	160
7.7.2	ServerConfiguration.....	161
7.7.3	ServerConfigurationType	161
7.7.4	UpdateCertificate.....	163
7.7.5	ApplyChanges	164
7.7.6	CreateSigningRequest.....	165
7.7.7	GetRejectedList.....	166
7.7.8	CertificateUpdatedAuditEventType	167
8	Gestion des KeyCredentials	168
8.1	Vue d'ensemble	168
8.2	Gestion en flux tiré.....	168
8.3	Gestion en flux poussé	169
8.4	Modèle d'information pour la gestion en flux tiré	170
8.4.1	Vue d'ensemble	170

8.4.2	KeyCredentialManagement.....	171
8.4.3	KeyCredentialServiceType.....	171
8.4.4	StartRequest	172
8.4.5	FinishRequest	173
8.4.6	Revoke	175
8.4.7	KeyCredentialAuditEventType	175
8.4.8	KeyCredentialRequestedAuditEventType.....	176
8.4.9	KeyCredentialDeliveredAuditEventType.....	176
8.4.10	KeyCredentialRevokedAuditEventType.....	177
8.5	Modèle d'information pour la gestion en flux poussé	177
8.5.1	Généralités	177
8.5.2	KeyCredentialConfiguration	178
8.5.3	KeyCredentialConfigurationType	178
8.5.4	UpdateCredential.....	179
8.5.5	DeleteCredential.....	180
8.5.6	KeyCredentialUpdatedAuditEventType	181
8.5.7	KeyCredentialDeletedAuditEventType	181
9	Services d'Autorisation	182
9.1	Vue d'ensemble	182
9.2	Cas d'utilisation implicite.....	183
9.3	Cas d'utilisation explicite.....	183
9.4	Cas d'utilisation chaîné	184
9.5	Modèle d'information pour la demande de jetons d'accès.....	185
9.5.1	Vue d'ensemble	185
9.5.2	AuthorizationServices	186
9.5.3	AuthorizationServiceType	186
9.5.4	RequestAccessToken	187
9.5.5	GetServiceDescription	188
9.5.6	AccessTokenIssuedAuditEventType	189
9.6	Modèle d'information pour la configuration de Serveurs	190
9.6.1	Vue d'ensemble	190
9.6.2	AuthorizationServices	190
9.6.3	AuthorizationServiceConfigurationType	190
Annexe A (informative)	Déploiement et configuration	192
A.1	Pare-feu et découverte	192
A.2	Résolution des références aux Serveurs distants	194
Annexe B (normative)	Constantes	196
Annexe C (normative)	Mapping d'OPC UA avec mDNS.....	197
C.1	Syntaxe des enregistrements de serveur DNS (SRV).....	197
C.2	Syntaxe des enregistrements de texte DNS (TXT)	198
C.3	Mapping des DiscoveryUrl	198
Annexe D (normative)	Identificateurs des fonctionnalités d'un Serveur.....	200
Annexe E (normative)	DirectoryServices	201
E.1	Découverte globale au moyen d'autres services d'annuaire.....	201
E.2	UDDI.....	202
E.3	LDAP	202
Annexe F (normative)	Serveur de découverte local	204
F.1	Présentation du répertoire de stockage des certificats	204

F.2	Répertoires d'installation sous Windows	205
Annexe G (normative)	Processus d'installation d'applications	206
G.1	Approvisionnement avec la gestion en flux tiré.....	206
G.2	Approvisionnement avec la gestion en flux poussé	206
G.3	Configuration des autorisations.....	207
Annexe H (informative)	Comparaison avec la RFC 7030	209
H.1	Vue d'ensemble	209
H.2	Obtention des certificats de CA.....	209
H.3	Inscription initiale.....	209
H.4	Redélivrance d'un certificat client.....	210
H.5	Génération de clés de serveur	210
H.6	Demande d'attributs CSR (Certificate Signing Request – demande de signature de certificat)	210
Figure 1	– Processus d'enregistrement auprès d'un LDS	118
Figure 2	– Processus de découverte simple	119
Figure 3	– Processus de découverte locale.....	120
Figure 4	– Processus de découverte de MulticastSubnet	120
Figure 5	– Processus de découverte globale.....	121
Figure 6	– Processus de découverte pour les Clients.....	122
Figure 7	– Relation entre le GDS et les autres composants	124
Figure 8	– Architecture à MulticastSubnet simple.....	125
Figure 9	– Architecture à MulticastSubnets multiples	125
Figure 10	– Architecture sans MulticastSubnet	126
Figure 11	– Espace d'adressage du GDS.....	127
Figure 12	– Modèle de gestion des certificats en flux tiré	138
Figure 13	– Modèle de gestion des certificats en flux poussé.....	139
Figure 14	– AddressSpace de gestion des certificats pour le GlobalDiscoveryServer	150
Figure 15	– AddressSpace pour le Serveur prenant en charge la gestion en flux poussé.....	161
Figure 16	– Modèle de gestion des KeyCredentials en flux tiré	169
Figure 17	– Modèle de gestion des KeyCredentials en flux poussé	170
Figure 18	– Espace d'Adressage utilisé pour la gestion des KeyCredentials en flux tiré	171
Figure 19	– AddressSpace utilisé pour la gestion des KeyCredentials en flux poussé	178
Figure 20	– Rôles et Services d'Autorisation	182
Figure 21	– Autorisation implicite	183
Figure 22	– Autorisation explicite	184
Figure 23	– Autorisation chaînée	185
Figure 24	– Modèle pour la demande de jetons d'accès auprès des Services d'Autorisation.....	186
Figure 25	– Modèle pour la configuration de Serveurs en vue d'utiliser les Services d'Autorisation.....	190
Figure A.1	– Serveurs de découverte à l'extérieur d'un pare-feu	192
Figure A.2	– Serveurs de découverte derrière un pare-feu	193
Figure A.3	– Utilisation d'un Serveur de Découverte avec un pare-feu	194
Figure A.4	– Suivi des références aux Serveurs distants.....	195

Figure E.1 – Processus de découverte globale UDDI ou LDAP	201
Figure E.2 – Structure d'un registre UDDI	202
Figure E.3 – Exemple de hiérarchie LDAP	203
Tableau 1 – Définition de l'Objet NamespaceMetadataType GDS	116
Tableau 2 – Définition de l'Objet Répertoire	127
Tableau 3 – Définition de DirectoryType	128
Tableau 4 – Définition de l'AddressSpace pour la Méthode FindApplications	129
Tableau 5 – Définition d'ApplicationRecordDataType	130
Tableau 6 – Définition de l'AddressSpace pour la Méthode RegisterApplication	131
Tableau 7 – Définition de l'AddressSpace pour la Méthode UpdateApplication	132
Tableau 8 – Définition de l'AddressSpace pour la Méthode UnregisterApplication	132
Tableau 9 – Définition de l'AddressSpace pour la Méthode GetApplication	133
Tableau 10 – Définition de l'AddressSpace pour la Méthode QueryApplications	135
Tableau 11 – Définition de l'AddressSpace pour la Méthode QueryServers	136
Tableau 12 – Définition d'ApplicationRegistrationChangedAuditEventType	137
Tableau 13 – Définition de TrustListType	141
Tableau 14 – Définition de l'AddressSpace pour la Méthode OpenWithMasks	142
Tableau 15 – Définition de l'AddressSpace pour la Méthode CloseAndUpdate	143
Tableau 16 – Définition de l'AddressSpace pour la Méthode AddCertificate	144
Tableau 17 – Définition de l'AddressSpace pour la Méthode RemoveCertificate	144
Tableau 18 – Définition de TrustListDataType	145
Tableau 19 – Valeurs de TrustListMasks	145
Tableau 20 – Définition de TrustListOutOfDateAlarmType	145
Tableau 21 – Définition de CertificateGroupType	146
Tableau 22 – Définition de CertificateType	147
Tableau 23 – Définition d'ApplicationCertificateType	147
Tableau 24 – Définition de HttpsCertificateType	147
Tableau 25 – Définition de UserCredentialCertificateType	148
Tableau 26 – Définition de RsaMinApplicationCertificateType	148
Tableau 27 – Définition de RsaSha256ApplicationCertificateType	148
Tableau 28 – Définition de CertificateGroupFolderType	149
Tableau 29 – Définition de TrustListUpdatedAuditEventType	149
Tableau 30 – Définition de l'ObjectType CertificateDirectoryType	151
Tableau 31 – Définition de l'AddressSpace pour la Méthode StartSigningRequest	153
Tableau 32 – Définition de l'AddressSpace pour la Méthode StartNewKeyPairRequest	155
Tableau 33 – Définition de l'AddressSpace pour la Méthode FinishRequest	156
Tableau 34 – Définition de l'AddressSpace pour la Méthode GetCertificateGroups	157
Tableau 35 – Définition de l'AddressSpace pour la Méthode GetTrustList	158
Tableau 36 – Définition de l'AddressSpace pour la Méthode GetCertificateStatus	159
Tableau 37 – Définition de CertificateRequestedAuditEventType	160
Tableau 38 – Définition de CertificateDeliveredAuditEventType	160
Tableau 39 – Définition de l'Objet ServerConfiguration	161

Tableau 40 – Définition de ServerConfigurationType	162
Tableau 41 – Définition de l'AddressSpace pour la Méthode UpdateCertificate	164
Tableau 42 – Définition de l'AddressSpace pour la Méthode ApplyChanges.....	165
Tableau 43 – Définition de l'AddressSpace pour la Méthode CreateSigningRequest	166
Tableau 44 – Définition de l'AddressSpace pour la Méthode GetRejectedList	167
Tableau 45 – Définition de CertificateUpdatedAuditEventType	167
Tableau 46 – Définition de l'Objet KeyCredentialManagement	171
Tableau 47 – Définition de KeyCredentialServiceType	172
Tableau 48 – Définition de l'AddressSpace pour la Méthode StartRequest.....	173
Tableau 49 – Définition de l'AddressSpace pour la Méthode FinishRequest.....	175
Tableau 50 – Définition de l'AddressSpace pour la Méthode Revoke	175
Tableau 51 – Définition de KeyCredentialAuditEventType	176
Tableau 52 – Définition de KeyCredentialRequestedAuditEventType	176
Tableau 53 – Définition de KeyCredentialDeliveredAuditEventType	177
Tableau 54 – Définition de KeyCredentialRevokedAuditEventType	177
Tableau 55 – Définition de l'Objet KeyCredentialConfiguration.....	178
Tableau 56 – Définition de KeyCredentialConfigurationType	179
Tableau 57 – Définition de l'AddressSpace pour la Méthode UpdateKeyCredential	180
Tableau 58 – Définition de l'AddressSpace pour la Méthode DeleteKeyCredential	181
Tableau 59 – Définition de KeyCredentialUpdatedAuditEventType	181
Tableau 60 – Définition de KeyCredentialUpdatedAuditEventType	182
Tableau 61 – Définition de l'Objet AuthorizationServices	186
Tableau 62 – Définition d'AuthorizationServiceType.....	187
Tableau 63 – Définition de l'AddressSpace pour la Méthode RequestAccessToken	188
Tableau 64 – Définition de l'AddressSpace pour la Méthode GetServiceDescription	189
Tableau 65 – Définition d'AccessTokenIssuedAuditEventType	189
Tableau 66 – Définition de l'Objet AuthorizationServices	190
Tableau 67 – Définition d'AuthorizationServiceConfigurationType	191
Tableau C.1 – Noms de services mDNS admis	197
Tableau C.2 – Format de chaîne des enregistrements TXT DNS.....	198
Tableau C.3 – Mapping des DiscoveryUrls avec les enregistrements SRV et TXT DNS	199
Tableau D.1 – Exemples de ServerCapabilityIdentifiers	200
Tableau E.1 – tModels UDDI.....	202
Tableau E.2 – Schéma des classes d'objets LDAP.....	203
Tableau F.1 – Présentation du répertoire de stockage des certificats d'application	204
Tableau H.1 – Vérification de l'autorisation d'un Serveur à fournir des certificats	209
Tableau H.2 – Vérification de l'autorisation d'un Client à demander des Certificats	209

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ARCHITECTURE UNIFIÉE OPC –

Partie 12: Services globaux et de découverte

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 62541-12 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.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65E/711/FDIS	65E/723/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 la série 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 "Termes et définitions" dans l'une des parties de la série IEC 62541.

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 *Architecture unifiée OPC*, 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.

ARCHITECTURE UNIFIÉE OPC –

Partie 12: Services globaux et de découverte

1 Domaine d'application

La présente partie de l'IEC 62541 spécifie la manière dont les *Clients* et les *Serveurs* de l'Architecture Unifiée OPC (OPC UA) interagissent avec les *DiscoveryServers* lorsqu'ils sont utilisés dans différents scénarios. Elle définit les exigences pour le *LocalDiscoveryServer*, le *LocalDiscoveryServer-ME* et le *GlobalDiscoveryServer*. Elle définit également les modèles d'information pour la gestion des *Certificats*, la gestion des *KeyCredentials* et les *Services d'Autorisation*.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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 62541-6, *Architecture unifiée OPC – Partie 6: Mappings*

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

IEC 62541-9, *Architecture unifiée OPC – Partie 9: Alarmes et Conditions*

IEC 62541-14, *Architecture unifiée OPC – Partie 14: PubSub*

X.500: ISO/IEC 9594-1:2017, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire – Partie 1: Aperçu général des concepts, modèles et services*

IETF RFC 1035, *DNS-Name: Domain Names – Implementation and Specification*
<http://www.ietf.org/rfc/rfc1035.txt>

IETF RFC 2986, *PKCS #10: Certification Request Syntax Specification*
<http://www.ietf.org/rfc/rfc2986.txt>

IETF RFC 3927, *Auto-IP: Dynamic Configuration of IPv4 Link-Local Addresses*
<http://www.ietf.org/rfc/rfc3927.txt>

IETF RFC 5958, *Asymmetric Key Packages*
<http://www.ietf.org/rfc/rfc5958.txt>

IETF RFC 6762, *mDNS: Multicast DNS*
<http://www.ietf.org/rfc/rfc6762.txt>

IETF RFC 6763, *DNS-SD: DNS Based Service Discovery*
<http://www.ietf.org/rfc/rfc6763.txt>

IETF RFC 7030, *Enrollment over Secure Transport*
<http://www.ietf.org/rfc/rfc7030.txt>

PKCS #12: *Personal Information Exchange Syntax*
<http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11301-wp-pkcs-12v1-1-personal-information-exchange-syntax.pdf>

DI: *OPC Unified Architecture for Devices (DI)*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-devices-di/>

ADI: *OPC Unified Architecture for Analyzer Devices (ADI)*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-analyzer-devices-adi/>

PLCopen: *OPC Unified Architecture / PLCopen Information Model*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-plcopen-information-model/>

FDI: *OPC Unified Architecture for FDI*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-fdi/>

ISA-95: *ISA-95 Common Object Model*
<https://opcfoundation.org/developer-tools/specifications-unified-architecture/isa-95-common-object-model/>