

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

---

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

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





## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 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  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://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 corrigendum or an amendment might have been published.

#### IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

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 It also gives information on projects, replaced and withdrawn publications.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](http://webstore.iec.ch/justpublished)

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

#### IEC Customer Service Centre - [webstore.iec.ch/csc](http://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: [sales@iec.ch](mailto:sales@iec.ch).

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

#### IEC Glossary - [std.iec.ch/glossary](http://std.iec.ch/glossary)

67 000 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.

---

### 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.

#### Recherche de publications IEC -

[webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)

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](http://webstore.iec.ch/justpublished)

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

#### Service Clients - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: [sales@iec.ch](mailto:sales@iec.ch).

#### Electropedia - [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

#### Glossaire IEC - [std.iec.ch/glossary](http://std.iec.ch/glossary)

67 000 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.



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>