

ANNEX A
REFERENCE DOCUMENTS

1. International
 - a. ACP 100, Allied Call Sign and Address Group System Instructions and Assignments
 - b. ACP 117, *Allied Routing Indicator Book*
 - c. ACP 120, “Common Security Protocol (CSP)”, final draft
 - d. ACP 123, *Common Messaging Strategy and Procedures*, November, 1994
 - e. ACP 127, *Communications Instructions - Tape Relay Procedures*
 - f. “CMI CONOPS”, draft
 - g. CCITT Recommendation E.123 (1988), *Notation for National and International Telephone numbers*
 - h. CCITT Recommendation F.1 (1992), *Operational provisions for the international public telegram service*
 - i. CCITT Recommendation F.200 (1992), *Teletex service*
 - j. CCITT Recommendation F.31 (1988), *Telegram Retransmission System*
 - k. CCITT Recommendation T.62 (1993), *Control procedures for teletex and Group 4 facsimile services*
 - l. CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications*
 - m. CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:1992, *Information technology - Open Systems Interconnection - Systems Management: Log control function*
 - n. CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*
 - o. ISO 3166-1: 1997, *Codes for the representation of names of countries and their subdivisions - part 1: Country codes*
 - p. ISO 7498-2: 1987, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*
 - q. ISO/IEC ISP 15125-0, “Information Technology - International Standardized Profile - Common upper layer requirements - For the Directory”, draft 1, 30 May 1996

- r. ISO/IEC ISP 15125-1, "Information Technology - International Standardized Profiles ADY11 - The Directory - DUA support of Directory Access Protocol", draft 8, 19 June 1998
- s. ISO/IEC ISP 15125-2, "Information Technology - International Standardized Profiles ADY12 - The Directory - DUA support of Distributed Operations", draft 6, 19 June 1998
- t. ISO/IEC ISP 15125-3, "Information Technology - International Standardized Profiles ADY21 - The Directory - DSA support of Directory Access Protocol", draft 5, 19 June 1998
- u. ISO/IEC ISP 15125-4, "Information Technology - International Standardized Profiles ADY22 - The Directory - DSA support of Distributed Operations", final draft, 20 January 1997
- v. ISO/IEC ISP 15125-5, "Information Technology - International Standardized Profiles ADY41 - The Directory - DUA Authentication as DAP initiator", draft 10, 19 June 1998
- w. ISO/IEC ISP 15125-6, "Information Technology - International Standardized Profiles ADY42 - The Directory - DSA Authentication as DAP responder", draft 8, 19 June 1998
- x. ISO/IEC ISP 15125-7, "Information Technology - International Standardized Profiles ADY43 - The Directory - DSA Authentication for DSP", draft 8, 22 July 1996
- y. ISO/IEC ISP 15125-9, "Information Technology - International Standardized Profiles ADY45 - The Directory - DSA Basic Access Control", draft 6, 24 July 1998
- z. ISO/IEC ISP 15125-10, "Information Technology - International Standardized Profiles ADY51 - The Directory - Shadowing using ROSE", draft 5, 12 July 1996
- aa. ISO/IEC ISP 15125-12, "Information Technology - International Standardized Profiles ADY53 - The Directory - Shadowing subset", draft 5, 12 July 1996
- bb. ISO/IEC ISP 15125-13, "Information Technology - International Standardized Profiles ADY61 - The Directory - Administrative areas", draft 4, 26 June 1998
- cc. ISO/IEC ISP 15125-14, "Information Technology - International Standardized Profiles ADY62 - The Directory - Establishment and utilization of shadowing agreements", draft 1, 17 Jan. 1997
- dd. ISO/IEC ISP 15125-15, "Information Technology - International Standardized Profiles ADY63 - Schema administration and publication", draft 3, 30 November, 1998
- ee. ISO/IEC ISP 15125-16, "Information Technology - International Standardized Profiles ADY71 - The Directory - Shadowing Operational Binding", draft 1, 30 July 1996
- ff. ISO/IEC ISP 15125-17, "Information Technology - International Standardized Profiles ADY72 - The Directory - Hierarchical Operational Binding", Internet draft, Dec. 1997
- gg. ISO/IEC ISP 15126-1, "Information Technology - International Standardized Profiles FDY11 - The Directory - Common Directory Use", draft 7, 17 July 1996

hh. ISO/IEC ISP 15126-2, “Information Technology - International Standardized Profiles FDY12 - The Directory - Directory System Schema”, draft 5, 17 July 1996

ii. ISO/IEC TR 10000-1: 1995, *Information Technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework*

jj. ISO/IEC TR 10000-2: 1995, *Information Technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and taxonomy for OSI profiles*

kk. ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2: 1996 *Information technology - Message Handling Systems (MHS) - Overall Architecture*

ll. ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1: 1995, *Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*

mm. ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2: 1995, *Information technology - Open Systems Interconnection - The Directory: Models*

nn. ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2: 1997, “Information technology - Open Systems Interconnection - The Directory: Models”

oo. ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8: 1995, *Information technology - Open Systems Interconnection - The Directory: Authentication framework*

pp. ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: 1997, “Information technology - Open Systems Interconnection - The Directory: Authentication framework”

qq. ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3: 1995, *Information technology - Open Systems Interconnection - The Directory: Abstract service definition*

rr. ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4: 1995, *Information technology - Open Systems Interconnection - The Directory: Procedures for distributed operation*

ss. ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5: 1995, *Information technology - Open Systems Interconnection - The Directory: Protocol specifications*

tt. ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6: 1995, *Information technology - Open Systems Interconnection - The Directory: Selected attribute types*

uu. ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6: 1997, “Information technology - Open Systems Interconnection - The Directory: Selected attribute types”

vv. ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7: 1995, *Information technology - Open Systems Interconnection - The Directory: Selected object classes*

ww.ITU-T Recommendation X.521 (1997) | ISO/IEC 9594-7: 1997, “Information technology - Open Systems Interconnection - The Directory: Selected object classes”

xx. ITU-T Recommendation X.525 (1993) | ISO/IEC 9594-9: 1995, *Information technology - Open Systems Interconnection - The Directory: Replication*

yy. ITU-T Recommendation X.530 (1997) | ISO/IEC 9594-10: 1997, “Information Technology - Open Systems Interconnection - The Directory: Use of Systems Management for Administration of the Directory”

zz. ITU-T Recommendation X.583(1997) | ISO/IEC 13248-1:1998, *Information Technology -- Open Systems Interconnection -- Directory Access Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

aaa.ITU-T Recommendation X.584(1997) | ISO/IEC 13248-2:1998, *Information Technology -- Open Systems Interconnection -- Directory System Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

bbb.ITU-T Recommendation X.585(1997) | ISO/IEC 13248-3:1998, *Information Technology -- Open Systems Interconnection -- Directory Operational Binding Management Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

ccc.ITU-T Recommendation X.586(1997) | ISO/IEC 13248-4:1998, *Information Technology -- Open Systems Interconnection -- Directory Information Shadowing Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

ddd.ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*

eee.ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Information object specification*

fff. ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification*

ggg.ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

hhh.ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3: 1996, *Information technology - Open Systems Interconnection - Security Frameworks in Open Systems - Access control framework*

iii. ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1: 1994, *Information technology - Remote Operations: Concepts, model and notation*

2. General

- a. Barker, P. and Kille, S., November 1991, “The COSINE and Internet X.500 Schema”, RFC 1274
- b. Boeyen, S., Howes, T., and Richard, P., September 1998, “Internet X.509 Public Key Infrastructure - LDAPv2 Schema”
- c. Mansfield, G. and Kille, S., January 1994, “X.500 Directory Monitoring MIB,” RFC 1567
- d. Smith, Mark, 17 November 1998, “Internet-Draft: Definition of the inetOrgPerson LDAP Object Class”

3. National

- a. Joint Chiefs of Staff, March 1983, Automatic Digital Network (AUTODIN) Operating Procedures, JANAP128(I)

4. Corrigenda to the X.500 Series of Recommendations | ISO/IEC 9594 not included in ISPs

5. Amendments to the X.500 Series of Recommendations | ISO/IEC 9594 not included in ISPs

- a. Final proposed Draft Amendments to Support the UTF8 Encoding of the ISO/IEC 10646 Character Set,” January 1998.
- b. ISO/IEC JTC 1 SC6 N11013, DAM to ISO/IEC Parts 7 and 8, The Directory - Amendments on Certificate Extensions, September 1998

ANNEX BSCHEMATABLE OF CONTENTSSECTION ICONCEPTS

1.	General.....	B-1
----	--------------	-----

SECTION IICOMMON STRUCTURAL OBJECT CLASSES AND NAME FORMS

2.	Common Structural Object Classes.....	B-1
3.	Directory Standard Structural Object Classes.....	B-2
a.	Base Object Classes	B-2
b.	Superclasses	B-2
c.	Other Standard Structural Object Classes	B-3
d.	Directory Standard Object Class Descriptions.....	B-3
e.	applicationEntity	B-3
f.	applicationProcess	B-4
g.	country.....	B-4
h.	cRLDistributionPoint	B-4
i.	device	B-5
j.	dSA.....	B-5
k.	groupOfNames	B-6
l.	groupOfUniqueNames	B-7
m.	locality.....	B-7
n.	organization.....	B-8
o.	organizationalPerson.....	B-8
p.	organizationalRole	B-9
q.	organizationalUnit.....	B-10
r.	residentialPerson.....	B-11
4.	MHS Standard Structural Object Classes.....	B-11
a.	mhs-distribution-list.....	B-11
b.	mhs-message-store	B-12
c.	mhs-message-transfer-agent	B-13
d.	mhs-user-agent	B-14
5.	ACP 133 Structural Object Classes.....	B-15
a.	Base Object Classes	B-15
b.	Superclasses	B-16
c.	aCPNetworkEdB.....	B-17
d.	aCPNetworkInstructionsEdB.....	B-17
e.	addressList.....	B-17

f.	aliasCommonName	B-18
g.	aliasOrganizationalUnit.....	B-19
h.	altSpellingACP127.....	B-19
i.	cadACP127	B-20
j.	distributionCodeDescription.....	B-21
k.	dSSCSPLA.....	B-21
l.	messagingGateway.....	B-22
m.	mLA	B-23
n.	mLAgent.....	B-24
o.	network.....	B-25
p.	networkInstructions	B-25
q.	orgACP127.....	B-26
r.	plaCollectiveACP127.....	B-26
s.	releaseAuthorityPerson.....	B-27
t.	releaseAuthorityPersonA	B-28
u.	routingIndicator.....	B-28
v.	sigintPLA	B-29
w.	sIPLA	B-30
x.	spotPLA.....	B-31
y.	taskForceACP127	B-31
z.	tenantACP127	B-32
6.	Name Forms and DIT Structural Rules.....	B-33

SECTION III

COMMON AUXILIARY OBJECT CLASSES AND ATTRIBUTES

7.	Common Auxiliary Object Classes.....	B-35
a.	Superclasses	B-35
b.	Other Standard Auxiliary Object Classes.....	B-35
c.	ACP 133-specific Auxiliary Object Classes	B-35
d.	certificationAuthority-V2.....	B-36
e.	deltaCRL	B-36
f.	distributionCodesHandled.....	B-36
g.	mhs-user.....	B-37
h.	otherContactInformation.....	B-37
i.	pkiCA.....	B-38
j.	pkiUser.....	B-38
k.	plaACP127	B-39
l.	plaData	B-39
m.	plaUser	B-40
n.	secure-user.....	B-40
o.	securePkiUser.....	B-41
p.	ukms	B-41
q.	userSecurityInformation.....	B-42
8.	Attributes in Common Content Object Classes.....	B-42
a.	Directory Standard Attributes	B-42
b.	MHS Standard Attributes.....	B-43

c.	RFC 1274-defined Attributes.....	B-43
d.	ACP 133-defined Attributes.....	B-44
e.	Other Standard Attributes.....	B-45
9.	Attributes Added by Content Rules	B-45
10.	Collective Attributes	B-46

SECTION IV

APPLYING CONTENT RULES IN THE COMMON CONTENT

11.	Common Content	B-47
12.	Directory Entries.....	B-51
a.	Address List Ed. A.....	B-51
b.	Address List Alias	B-51
c.	Alternate Spelling PLA	B-52
d.	Application Entity Ed. A.....	B-52
e.	Application Process.....	B-53
f.	CAD PLA.....	B-53
g.	Certification Authority Ed. B.....	B-53
h.	Country.....	B-53
i.	CRL Distribution Point	B-54
j.	Device Ed. A.....	B-54
k.	Distribution Code Description.....	B-54
l.	DSA Ed. A.....	B-55
m.	DSSCS PLA	B-55
n.	Group of Names.....	B-55
o.	Group of Unique Names	B-55
p.	Locality.....	B-56
q.	Messaging Gateway Ed. A.....	B-56
r.	Messaging Organizational Unit Alias	B-56
s.	MHS Distribution List.....	B-57
t.	MHS Message Store Ed. A.....	B-57
u.	MHS Message Transfer Agent Ed. A.....	B-58
v.	MHS User Agent.....	B-58
w.	MLA Ed. A.....	B-58
x.	Network Ed. B.....	B-59
y.	Network Instructions Ed. B.....	B-59
z.	Organization Ed. B.....	B-59
aa.	Organizational Person Ed. B.....	B-59
bb.	Organizational Person Alias	B-61
cc.	Organizational PLA.....	B-61
dd.	Organizational Role Ed. B	B-61
ee.	Organizational Role Alias	B-62
ff.	Organizational Unit Ed. B.....	B-63
gg.	Organizational Unit Alias.....	B-64
hh.	PLA Collective.....	B-64
ii.	Release Authority Person Ed. A.....	B-64
jj.	Release Authority Role Ed. B.....	B-65

kk.	Residential Person.....	B-66
ll.	Routing Indicator Ed. B	B-66
mm.	Signal Intelligence PLA.....	B-66
nn.	Special Intelligence PLA.....	B-66
oo.	SPOT PLA.....	B-67
pp.	Task Force PLA	B-67
qq.	Tenant PLA.....	B-67

SECTION V

OBJECT CLASSES HIERARCHY

13.	ACP 133-defined Object Classes	B-67
-----	--------------------------------------	------

SECTION VI

ATTRIBUTE TYPES HIERARCHY

14.	Attribute Subtypes.....	B-68
-----	-------------------------	------

SECTION VII

USEFUL OBJECT CLASSES AND NAME FORMS

15.	General.....	B-69
-----	--------------	------

SECTION VIII

USEFUL ATTRIBUTES

16.	General.....	B-70
-----	--------------	------

SECTION IX

ATTRIBUTE DEFINITIONS

17.	Common Content	B-70
18.	accessCodes.....	B-70
19.	accessSchema.....	B-70
20.	accountingCode.....	B-70
21.	aCPLegacyFormat.....	B-71
22.	aCPMobileTelephoneNumber.....	B-71
23.	aCPNetwAccessSchemaEdB	B-72
24.	aCPNetworkSchemaEdB	B-72
25.	aCPPagerTelephoneNumber	B-72
26.	aCPPreferredDelivery	B-72
27.	aCPTelephoneFaxNumber	B-72
28.	actionAddressees.....	B-74
29.	additionalAddressees.....	B-74
30.	additionalSecondPartyAddressees	B-74
31.	adminConversion.....	B-74
32.	administrator.....	B-74
33.	aigsExpanded	B-74

34.	aLExemptedAddressProcessor.....	B-74
35.	aliasedEntryName	B-75
36.	aliasPointer.....	B-75
37.	alid.....	B-75
38.	allowableOriginators	B-75
39.	aLReceiptPolicy.....	B-75
40.	alternateRecipient	B-75
41.	aLType	B-76
42.	aprUKMs.....	B-76
43.	associatedAL.....	B-76
44.	associatedOrganization.....	B-76
45.	associatedPLA.....	B-76
46.	attributeCertificate.....	B-76
47.	augUKMs	B-77
48.	authorityRevocationList.....	B-77
49.	buildingName.....	B-77
50.	businessCategory.....	B-77
51.	cACertificate	B-77
52.	certificateRevocationList	B-77
53.	cognizantAuthority.....	B-77
54.	commonName	B-78
55.	community.....	B-78
56.	copyMember.....	B-78
57.	countryName	B-78
58.	crossCertificatePair	B-78
59.	decUKMs	B-79
60.	deltaRevocationList.....	B-79
61.	deployed	B-79
62.	description.....	B-79
63.	destinationIndicator.....	B-79
64.	distinguishedName.....	B-80
65.	distributionCodeAction.....	B-80
66.	distributionCodeInfo	B-80
67.	dnQualifier	B-80
68.	dualRoute	B-80
69.	effectiveDate	B-80
70.	enhancedSearchGuide	B-81
71.	entryClassification.....	B-81
72.	expirationDate	B-81
73.	facsimileTelephoneNumber.....	B-81
74.	febUKMs.....	B-81
75.	garrison.....	B-81
76.	gatewayType	B-82
77.	generationQualifier.....	B-82
78.	ghpType.....	B-82
79.	givenName	B-82

80.	guard.....	B-83
81.	host.....	B-83
82.	hostOrgACP127	B-83
83.	houseIdentifier.....	B-83
84.	infoAddressees.....	B-83
85.	initials.....	B-83
86.	internationalISDNNumber.....	B-83
87.	janUKMs	B-84
88.	julUKMs.....	B-84
89.	junUKMs.....	B-84
90.	knowledgeInformation.....	B-84
91.	lastRecapDate.....	B-84
92.	listPointer	B-84
93.	lmf.....	B-84
94.	localityName	B-85
95.	longTitle	B-85
96.	mailDomains	B-85
97.	marUKMs.....	B-85
98.	mayUKMs	B-85
99.	member.....	B-85
100.	mhs-acceptable-eits	B-86
101.	mhs-deliverable-classes.....	B-86
102.	mhs-deliverable-content-types.....	B-86
103.	mhs-dl-archive-service.....	B-86
104.	mhs-dl-members.....	B-86
105.	mhs-dl-policy	B-86
106.	mhs-dl-related-lists.....	B-87
107.	mhs-dl-submit-permissions	B-87
108.	mhs-dl-subscription-service	B-87
109.	mhs-exclusively-acceptable-eits.....	B-87
110.	mhs-maximum-content-length.....	B-87
111.	mhs-message-store-dn.....	B-87
112.	mhs-or-addresses.....	B-88
113.	mhs-or-addresses-with-capabilities.....	B-88
114.	mhs-supported-attributes	B-88
115.	mhs-supported-automatic-actions	B-88
116.	mhs-supported-content-types.....	B-88
117.	mhs-supported-matching-rules.....	B-89
118.	mhs-unacceptable-eits	B-89
119.	militaryFacsimileNumber.....	B-89
120.	militaryTelephoneNumber	B-89
121.	minimize.....	B-89
122.	minimizeOverride.....	B-90
123.	name	B-90
124.	nameClassification.....	B-90
125.	nationality.....	B-90

126.	networkDN	B-90
127.	networkSchema	B-91
128.	novUKMs.....	B-91
129.	octUKMs	B-91
130.	onSupported	B-91
131.	operationName	B-91
132.	organizationalUnitName	B-91
133.	organizationName	B-92
134.	owner.....	B-92
135.	physicalDeliveryOfficeName	B-92
136.	plaAddressees.....	B-92
137.	plaNameACP127.....	B-93
138.	plaReplace	B-93
139.	plasServed	B-93
140.	positionNumber.....	B-93
141.	postalAddress.....	B-93
142.	postalCode.....	B-94
143.	postOfficeBox.....	B-94
144.	preferredDeliveryMethod.....	B-94
145.	presentationAddress.....	B-94
146.	primarySpellingACP127	B-95
147.	proprietaryMailboxes.....	B-95
148.	protocolInformation.....	B-95
149.	publish.....	B-95
150.	rank.....	B-95
151.	recapDueDate.....	B-95
152.	registeredAddress.....	B-95
153.	releaseAuthorityName	B-96
154.	remarks.....	B-96
155.	rfc822Mailbox.....	B-96
156.	rI.....	B-96
157.	rIClassification.....	B-96
158.	rIIInfo.....	B-96
159.	roleOccupant	B-97
160.	roomNumber	B-97
161.	searchGuide	B-97
162.	secondPartyAddressees	B-97
163.	section.....	B-97
164.	secureFacsimileNumber.....	B-97
165.	secureTelephoneNumber.....	B-98
166.	seeAlso	B-98
167.	sepUKMs.....	B-98
168.	serialNumber	B-98
169.	serviceNumber	B-98
170.	serviceOrAgency.....	B-98
171.	sHD.....	B-99

172.	shortTitle	B-99
173.	sigad	B-99
174.	spot	B-99
175.	stateOrProvinceName	B-99
176.	streetAddress	B-99
177.	supportedAlgorithms	B-100
178.	supportedApplicationContext	B-100
179.	surname	B-100
180.	tARE	B-100
181.	tCC	B-100
182.	tCCG	B-100
183.	telephoneNumber	B-100
184.	teletexTerminalIdentifier	B-101
185.	telexNumber	B-101
186.	title	B-101
187.	transferStation	B-101
188.	tRC	B-101
189.	uniqueIdentifier	B-102
190.	uniqueMember	B-102
191.	usdConversion	B-102
192.	userCertificate	B-102
193.	userPassword	B-102
194.	x121Address	B-103
195.	Useful	B-103
a.	hoursOfOperation	B-103
b.	jpegPhoto	B-103
c.	militaryPostalAddress	B-103
d.	visitorAddress	B-103

SECTION X

DIRECTORY SYSTEM SCHEMA

196.	General	B-104
197.	Standard Subentry Object Classes	B-104
198.	Standard Operational Attributes	B-104
a.	Directory Operational Attributes	B-105
b.	DSA Specific Entry (DSE) Operational Attributes	B-106
199.	Rules for DIT Schema Management	B-107

SECTION XI

NATIONAL DIRECTORY INFORMATION TREES

200.	Australian DIT	B-109
201.	Canadian DIT	B-109
202.	New Zealand DIT	B-110
203.	United Kingdom DIT	B-111
204.	United States DIT	B-112

a.	Top-Level.....	B-113
b.	Service/Agency/Command Subtrees.....	B-113

SECTION XII

ACP 133 DATA TYPES

205.	Example Content Rules.....	B-119
a.	aCPApplicationEntityRuleEdA.....	B-120
b.	aCPCRLDistributionPointRule	B-121
c.	aCPDeviceRuleEdA.....	B-121
d.	aCPDSARuleEdA	B-121
e.	aCPGroupOfNamesRule	B-121
f.	aCPLocalityRule	B-121
g.	aCPMhs-distribution-listRule.....	B-122
h.	aCPMhs-message-storeRuleEdA.....	B-122
i.	aCPMhs-message-transfer-agentRuleEdA.....	B-122
j.	aCPMhs-user-agentRule.....	B-122
k.	aCPOrganizationalPersonRuleEdB.....	B-122
l.	aCPOrganizationalRoleRuleEdB.....	B-123
m.	aCPOrganizationalUnitRuleEdB.....	B-123
n.	aCPOrganizationRuleEdB.....	B-124
o.	aCPRoutingIndicatorRuleEdB.....	B-124
p.	addressListRuleEdA.....	B-124
q.	aliasCommonNameRule.....	B-125
r.	aliasOrganizationalUnitRule	B-125
s.	distributionCodeDescriptionRule.....	B-125
t.	messagingGatewayRuleEdA.....	B-125
u.	mLAgentRule.....	B-126
v.	networkEdBRule	B-126
w.	networkInstructionsEdBRule	B-126
x.	rAPersonRuleEdA.....	B-126
y.	sigtintPLARule.....	B-126
z.	spotPLARule	B-127
206.	Common Content ASN.1 Definitions	B-127
207.	Common Content Module	B-127
a.	structural object classes.....	B-128
(1)	aCPNetworkEdB.....	B-129
(2)	aCPNetworkInstructionsEdB.....	B-129
(3)	addressList.....	B-129
(4)	aliasCommonName	B-129
(5)	aliasOrganizationalUnit.....	B-130
(6)	altSpellingACP127.....	B-130
(7)	cadACP127	B-130
(8)	distributionCodeDescription.....	B-130
(9)	dSSCSPLA.....	B-130
(10)	messagingGateway.....	B-131
(11)	mLA	B-131

(12)	mLAgent.....	B-131
(13)	network.....	B-132
(14)	networkInstructions	B-132
(15)	orgACP127.....	B-132
(16)	plaCollectiveACP127.....	B-133
(17)	releaseAuthorityPerson.....	B-133
(18)	releaseAuthorityPersonA	B-133
(19)	routingIndicator.....	B-134
(20)	sigintPLA	B-134
(21)	sIPLA	B-134
(22)	spotPLA.....	B-135
(23)	taskForceACP127	B-135
(24)	tenantACP127	B-135
b.	auxiliary object classes.....	B-135
(1)	distributionCodesHandled.....	B-136
(2)	otherContactInformation.....	B-136
(3)	plaACP127	B-136
(4)	plaData	B-136
(5)	plaUser	B-137
(6)	secure-user.....	B-137
(7)	securePkiUser.....	B-137
(8)	ukms	B-137
c.	attribute types	B-138
(1)	accessCodes.....	B-138
(2)	accessSchema.....	B-138
(3)	accountingCode.....	B-138
(4)	aCPLegacyFormat.....	B-138
(5)	aCPMobileTelephoneNumber.....	B-139
(6)	aCPNetwAccessSchemaEdB	B-139
(7)	aCPNetworkSchemaEdB	B-139
(8)	aCPPagerTelephoneNumber	B-139
(9)	aCPPREFERREDDELIVERY	B-139
(10)	aCPTelephoneFaxNumber	B-139
(11)	actionAddressees.....	B-140
(12)	additionalAddressees.....	B-140
(13)	additionalSecondPartyAddressees	B-140
(14)	adminConversion	B-140
(15)	administrator.....	B-140
(16)	aigsExpanded	B-140
(17)	aLEXemptedAddressProcessor	B-141
(18)	aliasPointer.....	B-141
(19)	alid	B-141
(20)	allowableOriginators	B-141
(21)	aLReceiptPolicy	B-141
(22)	alternateRecipient	B-141
(23)	aLType	B-142

(24)	aprUKMs.....	B-142
(25)	associatedAL.....	B-142
(26)	associatedOrganization.....	B-142
(27)	associatedPLA.....	B-142
(28)	augUKMs	B-142
(29)	cognizantAuthority.....	B-143
(30)	community.....	B-143
(31)	copyMember.....	B-143
(32)	decUKMs	B-143
(33)	deployed	B-143
(34)	distributionCodeAction.....	B-143
(35)	distributionCodeInfo	B-144
(36)	dualRoute	B-144
(37)	effectiveDate	B-144
(38)	entryClassification.....	B-144
(39)	expirationDate	B-144
(40)	febUKMs.....	B-144
(41)	garrison.....	B-145
(42)	gatewayType	B-145
(43)	ghpType.....	B-145
(44)	guard.....	B-145
(45)	hostOrgACP127	B-145
(46)	infoAddressees.....	B-145
(47)	janUKMs	B-146
(48)	julUKMs.....	B-146
(49)	junUKMs.....	B-146
(50)	lastRecapDate.....	B-146
(51)	listPointer	B-146
(52)	lmf.....	B-146
(53)	longTitle	B-147
(54)	mailDomains	B-147
(55)	marUKMs.....	B-147
(56)	mayUKMs	B-147
(57)	militaryFacsimileNumber.....	B-147
(58)	militaryTelephoneNumber.....	B-147
(59)	minimize.....	B-148
(60)	minimizeOverride.....	B-148
(61)	nameClassification.....	B-148
(62)	nationality.....	B-148
(63)	networkDN	B-148
(64)	networkSchema	B-148
(65)	novUKMs.....	B-149
(66)	octUKMs	B-149
(67)	onSupported	B-149
(68)	operationName	B-149
(69)	plaAddressees.....	B-149

(70)	plaNameACP127.....	B-149
(71)	plaReplace	B-150
(72)	plasServed	B-150
(73)	positionNumber.....	B-150
(74)	primarySpellingACP127	B-150
(75)	proprietaryMailboxes.....	B-150
(76)	publish.....	B-150
(77)	rank	B-151
(78)	recapDueDate.....	B-151
(79)	releaseAuthorityName	B-151
(80)	remarks.....	B-151
(81)	rI	B-151
(82)	rIClassification.....	B-152
(83)	rIInfo.....	B-152
(84)	secondPartyAddressees	B-152
(85)	section.....	B-152
(86)	secureFacsimileNumber.....	B-152
(87)	secureTelephoneNumber.....	B-152
(88)	sepUKMs.....	B-153
(89)	serviceNumber	B-153
(90)	serviceOrAgency.....	B-153
(91)	sHD.....	B-153
(92)	shortTitle	B-153
(93)	sigad	B-153
(94)	spot	B-154
(95)	tARE.....	B-154
(96)	tCC	B-154
(97)	tCCG	B-154
(98)	transferStation.....	B-154
(99)	tRC	B-155
(100)	usdConversion.....	B-155
d.	collective attributes	B-155
(1)	collective-mhs-or-addresses.....	B-155
(2)	collectiveMilitaryFacsimileNumber.....	B-155
(3)	collectiveMilitaryTelephoneNumber.....	B-155
(4)	collectiveNationality	B-155
(5)	collectiveSecureFacsimileNumber.....	B-156
(6)	collectiveSecureTelephoneNumber	B-156
e.	name forms.....	B-156
(1)	aCPNetworkEdBNameForm.....	B-156
(2)	aCPNetworkInstrEdBNameForm.....	B-156
(3)	addressListNameForm.....	B-156
(4)	aENameForm.....	B-156
(5)	aliasCNNameForm.....	B-157
(6)	aliasOUNameForm.....	B-157
(7)	alternateSpellingPLANNameForm.....	B-157

(8)	cadPLANameForm.....	B-157
(9)	distributionCodeDescriptionNameForm.....	B-157
(10)	dSSCSPLANameForm.....	B-157
(11)	messagingGatewayNameForm.....	B-158
(12)	mhs-dLNameForm.....	B-158
(13)	mLANameForm.....	B-158
(14)	mLAgentNameForm.....	B-158
(15)	mSNameForm.....	B-158
(16)	mTANameForm.....	B-158
(17)	mUANameForm.....	B-159
(18)	networkNameForm.....	B-159
(19)	networkInstructionsNameForm.....	B-159
(20)	organizationalPLANameForm.....	B-159
(21)	organizationNameForm.....	B-159
(22)	orgRNameForm.....	B-159
(23)	orgUNameForm.....	B-160
(24)	plaCollectiveNameForm.....	B-160
(25)	qualifiedOrgPersonNameForm.....	B-160
(26)	releaseAuthorityPersonNameForm.....	B-160
(27)	releaseAuthorityPersonANameForm.....	B-160
(28)	routingIndicatorNameForm.....	B-160
(29)	sigintPLANameForm.....	B-161
(30)	sIPLANameForm.....	B-161
(31)	spotPLANameForm.....	B-161
(32)	taskForcePLANameForm.....	B-161
(33)	tenantPLANameForm.....	B-161
f.	miscellaneous data types	B-162
g.	object identifiers	B-163
208.	Useful Attributes ASN.1 Definitions	B-167
209.	Useful Attributes Module.....	B-168
a.	hoursOfOperation.....	B-168
b.	jpegPhoto.....	B-168
c.	militaryPostalAddress	B-168
d.	visitorAddress.....	B-169
e.	collectiveMilitaryPostalAddress	B-169
f.	collectiveVisitorAddress	B-169

List of Figures

Figure B-1: Hierarchy of Common Content Object Classes.....	B-67
Figure B-2: Attribute Types Defined by Subtyping.....	B-68
Figure B-3: Australian Top-Level DIT.....	B-109
Figure B-4: Canadian Top-Level DIT	B-110
Figure B-5: New Zealand Top-Level DIT	B-111
Figure B-6: UK Top-Level DIT	B-112
Figure B-7: U.S. Top-Level DIT	B-113
Figure B-8: U.S. DIT Subtrees for Each Service/Agency/Command.....	B-114
Figure B-9: U.S. DIT Locations Subtree	B-115
Figure B-10: U.S. DIT Organizations Subtree.....	B-115
Figure B-11: Example Army Locations Directory Entries	B-116
Figure B-12: Example Army Organizations Directory Entries	B-117
Figure B-13: Example PACOM Combined Task Force Directory Entries	B-118

List of Tables

Table B-1: applicationEntity Object Class.....	B-3
Table B-2: applicationProcess Object Class	B-4
Table B-3: country Object Class	B-4
Table B-4: cRLDistributionPoint Object Class	B-5
Table B-5: device Object Class.....	B-5
Table B-6: dSA Object Class	B-6
Table B-7: groupOfNames Object Class	B-7
Table B-8: locality Object Class	B-7
Table B-9: organization Object Class	B-8
Table B-10: organizationalPerson Object Class	B-9
Table B-11: organizationalRole Object Class.....	B-10
Table B-12: organizationalUnit Object Class	B-11
Table B-13: mhs-distribution-list Object Class	B-12
Table B-14: mhs-message-store Object Class	B-13
Table B-15: mhs-message-transfer-agent Object Class	B-14
Table B-16: mhs-user-agent Object Class	B-15
Table B-17: aCPNetworkEdB Object Class	B-17
Table B-18: aCPNetworkInstructionsEdB Object Class	B-17
Table B-19: addressList Object Class.....	B-18
Table B-20: aliasCommonName Object Class	B-19
Table B-21: aliasOrganizationalUnit Object Class	B-19
Table B-22: altSpellingACP127 Object Class	B-20
Table B-23: cadACP127 Object Class.....	B-20
Table B-24: distributionCodeDescription Object Class.....	B-21
Table B-25: dSSCSPLA Object Class	B-22
Table B-26: messagingGateway Object Class	B-23
Table B-27: mLAgent Object Class.....	B-24
Table B-28: mLAgent Object Class.....	B-24
Table B-29: network Object Class.....	B-25
Table B-30: networkInstructions Object Class	B-25
Table B-31: orgACP127 Object Class	B-26
Table B-32: plaCollectiveACP127 Object Class	B-27
Table B-33: releaseAuthorityPerson Object Class.....	B-28
Table B-34: releaseAuthorityPersonA Object Class	B-28
Table B-35: routingIndicator Object Class	B-29
Table B-36: sigintPLA Object Class.....	B-30
Table B-37: sIPLA Object Class	B-30
Table B-38: spotPLA Object Class	B-31
Table B-39: taskForceACP127 Object Class.....	B-32
Table B-40: tenantACP127 Object Class.....	B-33
Table B-41: Name Forms.....	B-33
Table B-42: certificationAuthority-V2 Object Class	B-36
Table B-43: distributionCodesHandled Object Class	B-37
Table B-44: mhs-user Object Class.....	B-37

Table B-45: otherContactInformation Object Class.....	B-38
Table B-46: pkiCA Object Class.....	B-38
Table B-47: pkiUser Object Class.....	B-39
Table B-48: plaACP127 Object Class.....	B-39
Table B-49: plaData Object Class.....	B-40
Table B-50: plaUser Object Class.....	B-40
Table B-51: secure-user Object Class	B-41
Table B-52: securePkiUser Object Class	B-41
Table B-53: ukms Object Class.....	B-42
Table B-54: Common Content	B-49
Table B-55: DSE Types and Their Purpose.....	B-107

SECTION I

CONCEPTS

1. General

- a. The ACP 133 schema is based to the extent possible on civilian standards, in particular, ITU-T Rec. X.402 (1995), ITU-T Rec. X.509 (1993), ITU-T Rec. X.520 (1993), and ITU-T Rec. X.521 (1993) plus the 1997 operational security and certificate extensions to ITU-T Rec. X.509, ITU-T Rec. X.520 and ITU-T Rec. X.521. Several object classes have been introduced that are included in the Certificate Extensions DAM 1 to ISO/IEC 9594 Parts 7 & 8 (i.e., X.521 & X.509) that is being applied to the 1997 Directory Standards. In the Allied Directory System, all of the object classes, attributes, matching rules, and name forms defined in X.501, X.509, X.520, X.521, X.402, and the DAM shall be implemented.
- b. This ACP defines a “common content” which is the schema that must be implemented for the Allied Directory System. Each directory entry in the Allied Directory System is defined by a structural object class and, potentially, a content rule. The content rule includes the structural object class, allowed auxiliary object classes, and additional attributes.
- c. Examples of content rules are given in Section IV of this annex. Inclusion of auxiliary object classes and additional attributes depends on the application, as specified in Chapter 3. For example, an entry for an organizational unit which does secure ACP 123 messaging would include the mhs-user and securePkiUser auxiliary object classes. An organizational unit which is used for DIT navigational purposes would not populate those classes.
- d. Each country may construct a content rule based on a structural object class and may include additional auxiliary object classes and more attributes as long as at least the Common Content is supported.
- e. Besides the Common Content, this annex also contains definitions of generally useful object classes and attributes.

SECTION II

COMMON STRUCTURAL OBJECT CLASSES AND NAME FORMS

2. Common Structural Object Classes

The Allied Common Content includes standard structural object classes and structural object classes defined in this ACP. The Allied Directory System entries defined using these structural object classes are described in Section IV of this annex.

3. Directory Standard Structural Object Classes

a. Base Object Classes

Although all of the directory standard structural object classes shall be supported for the Allied Directory System, the Common Content uses only the following standard classes as the structural object classes of Allied Directory Entries:

- applicationEntity
- applicationProcess
- country
- cRLDistributionPoint
- device
- dSA
- groupOfNames
- locality
- organization
- organizationalPerson
- organizationalRole
- organizationalUnit

b. Superclasses

Each of these standard classes is used in the Common Content as a superclass in the definition of a standard structural object class, as described below, or of a structural object class defined in this ACP:

- alias
- applicationEntity
- mhs-message-transfer-agent
- person
- pkiUser

- strongAuthenticationUser
 - top
- c. Other Standard Structural Object Classes

There are several other standard structural object classes that are included in the Common Content, but which are not used to meet Allied Directory requirements. These structural object classes are:

- groupOfUniqueNames
 - residentialPerson
- d. Directory Standard Object Class Descriptions

The rest of this paragraph describes the directory standard structural object classes that are used as base classes in directory entries in the Common Content. Descriptions are not included for the object classes that are used solely as superclasses (e.g., person) in the Common Content.

e. applicationEntity

The applicationEntity object class is used to define directory entries representing application entities. An application entity consists of those aspects of an application process pertinent to communications. If an application entity is represented as a Directory object distinct from an application process, the commonName attribute is used to carry the value of the application entity qualifier. Table B-1 shows the composition of the applicationEntity object class. This object class is the base class for Application Entity Ed. A and Certification Authority Ed. B (see paragraph 12 g.) type directory entries and is the superclass of the base class for DSA Ed. A, MHS Message Store Ed. A, MHS Message Transfer Agent Ed. A, MHS User Agent, and MLA Ed. A type directory entries.

Table B-1
applicationEntity Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: presentationAddress	m
X.520: seeAlso	o
X.520: supportedApplicationContext	o

f. applicationProcess

The applicationProcess object class is used to define directory entries representing application processes. An application process is an element within a computer system which performs the information processing for a particular application. Table B-2 shows the composition of the applicationProcess object class. This object class is the base class for Application Process type directory entries.

Table B-2
applicationProcess Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: seeAlso	o

g. country

The country object class is used to define nation directory entries. Table B-3 shows the composition of the country object class. This object class is the base class for Country type directory entries.

Table B-3
country Object Class

Attribute	m/o
X.520: countryName	m
X.520: description	o
X.520: searchGuide	o

h. cRLDistributionPoint

The cRLDistributionPoint object class is used in defining directory entries for objects which act as CRL Distribution Points as defined in ITU-T Rec. X.521 | ISO/IEC 9594-7. Table

B-4 shows the composition of the cRLDistributionPoint object class. This object class is the base class for CRL Distribution Point type directory entries.

Table B-4
cRLDistributionPoint Object Class

Attribute	m/o
X.509: authorityRevocationList	o
X.509: certificateRevocationList	o
X.520: commonName	m
X.509-1997: deltaRevocationList	o

i. device

The device object class is used to define entries representing devices. A device is a physical unit which can communicate, such as a modem, disk drive, etc. Table B-5 shows the composition of the device object class. This object class is the base class for Device Ed. A type directory entries.

Table B-5
device Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o*
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o*
X.520: seeAlso	o
X.520: serialNumber	o*

* At least one of localityName, serialNumber, owner, should be included. The choice is dependent on device type.

j. dSA

The dSA object class is used to define directory entries representing application entities that implement the X.500 DSA functionality. A DSA is as defined in ITU-T Rec. X.501

| ISO/IEC 9594-2. Table B-6 shows the composition of the dSA object class. This object class is the base class for DSA Ed. A type directory entries.

Table B-6
dSA Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: knowledgeInformation	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

k. groupOfNames

The groupOfNames object class is used to define directory entries representing an unordered set of names which represent individual objects or other groups of names. The membership of a group is static, i.e., it is explicitly modified by administrative action, rather than dynamically determined each time the group is referred to. The membership of a group can be reduced to a set of individual object's names by replacing each group with its membership. This process would be carried out recursively until all constituent group names have been eliminated, and only the names of individual objects remain. Table B-7 shows the composition of the groupOfNames object class. This object class is the base class for Group of Names type directory entries.

Table B-7
groupOfNames Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: commonName	m
X.520: description	o
X.520: member	m
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
X.520: seeAlso	o

l. groupOfUniqueNames

The groupOfUniqueNames object class is not used for Allied Directory entries, but is described in X.521.

m. locality

The locality object class is used to define directory entries that represent places. Table B-8 shows the composition of the locality object class. This object class is the base class for Locality type directory entries.

Table B-8
locality Object Class

Attribute	m/o
X.520: description	o
X.520: localityName	o*
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o*
X.520: streetAddress	o

* At least one of localityName or stateOrProvinceName must be present.

n. organization

The organization object class is used to define directory entries that represent organizations. Table B-9 shows the composition of the organization object class. This object class is the base class for Organization Ed. B and Certification Authority Ed. B (see paragraph 12 g in this annex.) type directory entries.

Table B-9
organization Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationName	m
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.509: userPassword	o
X.520: x121Address	o

o. organizationalPerson

The organizationalPerson object class is used to define directory entries representing people employed by, or in some other important way associated with, an organization. Table B-10 shows the composition of the organizationalPerson object class. This object class is the base class for Organizational Person Ed. B type directory entries.

Table B-10
organizationalPerson Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: seeAlso*	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: surname*	m
X.520: telephoneNumber*	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.520: title	o
X.509: userPassword*	o
X.520: x121Address	o

* from person (superclass)

p. organizationalRole

The organizationalRole object class is used to define directory entries representing positions or roles within an organization. An organizational role is normally considered to be filled by a particular organizational person. Over its lifetime, however, an organizational role may be filled by a number of different organizational persons in succession. In general, an organizational role may be filled by a person or a non-human entity. Table B-11 shows the composition of the organizationalRole object class. This object class is the base class for Organizational Role Ed. B, Release Authority Role Ed. B, and Certification Authority Ed. B (see paragraph 12 g) type directory entries.

Table B-11
organizationalRole Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: roleOccupant	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.520: x121Address	o

q. organizationalUnit

The organizationalUnit object class is used to define directory entries representing subdivisions of organizations. Table B-12 shows the composition of the organizationalUnit object class. This object class is the base class for Organizational Unit Ed. B and Certification Authority Ed. B (see paragraph 12 g.) type directory entries.

Table B-12
organizationalUnit Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	m
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.509: userPassword	o
X.520: x121Address	o

r. residentialPerson

The residentialPerson object class is not used for Allied Directory entries, but is described in X.521.

4. MHS Standard Structural Object Classes

All of the structural object classes in ITU-T Rec. X.402 | ISO/IEC 10021-2 are used in the Common Content.

a. mhs-distribution-list

The mhs-distribution-list object class is used to define a directory entry that represents a distribution list (DL), that is, an address list that is expanded by the MTS. The attributes in the entry identify the distribution list name, submit permissions, and OR-addresses and, to the extent that the relevant attributes are present, describe the DL, identify its organization, organizational units, and owner; cite related objects; identify its maximum content

length, deliverable content types, and acceptable, exclusively acceptable, and unacceptable encoded information types (EITs); and identify its expansion policy, subscription addresses, archive addresses, related lists and members. Table B-13 shows the composition of the mhs-distribution-list object class. This object class is the base class for MHS Distribution List type directory entries.

Table B-13
mhs-distribution-list Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-dl-archive-service	o
X.402: mhs-dl-members	o
X.402: mhs-dl-policy	o
X.402: mhs-dl-related-lists	o
X.402: mhs-dl-submit-permissions	m
X.402: mhs-dl-subscription-service	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-or-addresses	m
X.402: mhs-unacceptable-eits	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
X.520: seeAlso	o

b. mhs-message-store

The mhs-message-store object class is used to define directory entries that represent application entities that implement the MHS MS functionality. The attributes in an entry, to the extent that they are present, describe the MS, identify its owner, and enumerate the attributes, automatic actions, matching rules, content types, and network protocols the MS supports. Table B-14 shows the composition of the mhs-message-store object class. This object class is the base class for MHS Message Store Ed. A type directory entries.

Table B-14
mhs-message-store Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-supported-attributes	o
X.402: mhs-supported-automatic-actions	o
X.402: mhs-supported-content-types	o
X.402: mhs-supported-matching-rules	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

c. mhs-message-transfer-agent

The mhs-message-transfer-agent object class is used to define directory entries that represent application entities that implement the MHS MTA functionality. The attributes in an entry, to the extent that they are present, describe the MTA and identify its owner, the maximum content length it can handle, and its supported network protocols. Table B-15 shows the composition of the mhs-message-transfer-agent object class. This object class is the base class for MHS Message Transfer Agent Ed. A type directory entries and is the superclass of the base class for Messaging Gateway Ed. A type directory entries.

Table B-15
mhs-message-transfer-agent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-maximum-content-length	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

d. mhs-user-agent

The mhs-user-agent object class is used to define directory entries that represent application entities that implement the MHS UA functionality. The attributes in an entry, to the extent that they are present, identify the UA's owner; the maximum content length, content types, and EITs it can handle; its deliverable classes; its OR-address; and its supported network protocols. Table B-16 shows the composition of the mhs-user-agent object class. This object class is the base class for MHS User Agent type directory entries.

Table B-16
mhs-user-agent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-classes	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-or-addresses	o
X.402: mhs-unacceptable-eits	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

5. ACP 133 Structural Object Classes

a. Base Object Classes

The structural object classes of Allied Directory Entries, specified in this annex, for Common Content are:

- aCPNetworkEdB
- aCPNetworkInstructionsEdB
- addressList
- aliasCommonName
- aliasOrganizationalUnit
- altSpellingACP127
- cadACP127

- distributionCodeDescription
- dSSCSPLA
- messagingGateway
- mLAn
- mLAgent
- network
- networkInstructions
- orgACP127
- plaCollectiveACP127
- releaseAuthorityPerson
- releaseAuthorityPersonA
- routingIndicator
- sigintPLA
- sIPLA
- spotPLA
- taskForceACP127
- tenantACP127

b. Superclasses

Each of these auxiliary object classes, specified in this ACP (see paragraph 7), is used in the Common Content as a superclass in the definition of a structural object class defined in this ACP:

- plaACP127
- plaData
- secure-user
- securePkiUser

c. aCPNetworkEdB

The aCPNetworkEdB structural object class is used to define directory entries representing interconnected communications networks. This object class replaces the network object class. Table B-17 shows the composition of the aCPNetworkEdB object class. This is the base class for Network EdB type directory entries. A Network EdB entry can have subordinate entries that define the access and instructions for reaching other networks.

Table B-17
aCPNetworkEdB Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
ACP 133: aCPNetworkSchemaEdB	o
ACP 133: operationName	o
X.520: seeAlso	o

d. aCPNetworkInstructionsEdB

The aCPNetworkInstructionsEdB structural object class is used to define a directory entry that provides the description of how to reach the subject network from another network. Table B-18 shows the composition of the aCPNetworkInstructionsEdB object class. This object class is the base class for Network Instructions EdB type directory entries.

Table B-18
aCPNetworkInstructionsEdB Object Class

Attribute	m/o
ACP 133: accessCodes	o
ACP 133: aCPNetwAccessSchemaEdB	o
X.520: commonName*	m
X.520: description*	o
ACP 133: networkDN	o

e. addressList

The addressList object class is used to define directory entries that represent address lists, in particular, the members of the list. The sender of a message uses the address list name to

send to all of the members in the list. The replacement of the address list name by the members of the list is performed by the sending UA or an MLA, instead of the MTS. Table B-19 shows the composition of the addressList object class. This object class is the base class for Address List Ed. A type directory entries.

Table B-19
addressList Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: commonName	m
ACP 133: copyMember	o
X.520: description	o
X.520: member	o
X.402: mhs-dl-archive-service	o
X.402: mhs-dl-policy	o
X.402: mhs-dl-related-lists	o
X.402: mhs-dl-submit-permissions	m
X.402: mhs-dl-subscription-service	o
ACP 133: aLEXemptedAddressProcessor	o
ACP 133: alid	o
ACP 133: aLReceiptPolicy	o
ACP 133: aLType	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
ACP 133: remarks	o
X.520: seeAlso	o

f. aliasCommonName

The aliasCommonName object class is used for an alias entry named by commonName. This permits, for example, an additional name to be given to a person, role, or address list. Table B-20 shows the composition of the aliasCommonName object class. This object class is the base class for Address List Alias, Organizational Person Alias, and Organizational Role Alias type directory entries.

Table B-20
aliasCommonName Object Class

Attribute	m/o
X.501: aliasedEntryName*	m
X.520: commonName	m

* from alias (superclass)

g. aliasOrganizationalUnit

The aliasOrganizationalUnit object class is used for an alias entry named by organizationalUnit. This permits an additional name to be given to a suborganization. Table B-21 shows the composition of the aliasOrganizationalUnit object class. This object class is the base class for Messaging Organizational Unit Alias and Organizational Unit Alias type directory entries.

Table B-21
aliasOrganizationalUnit Object Class

Attribute	m/o
X.501: aliasedEntryName*	m
X.520: organizationalUnitName	m

* from alias (superclass)

h. altSpellingACP127

The altSpellingACP127 object class is used to represent an alternative spelling for a PLA and always contains a reference to the PLA for which it provides an alternate spelling. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-22 shows the composition of the altSpellingACP127 object class. This object class is the base class for Alternate Spelling PLA type directory entries.

Table B-22
altSpellingACP127 Object Class

Attribute	m/o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: plaReplace	m
ACP 133: primarySpellingACP127	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

i. cadACP127

The cadACP127 (Collective Address Designator) object class is used to represent an ACP 127/JANAP 128 distribution list. It is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-23 shows the composition of the cadACP127 object class. This object class is the base class for CAD PLA type directory entries.

Table B-23
cadACP127 Object Class

Attribute	m/o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	o
ACP 133: remarks*	o
ACP 133: rInfo	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

j. distributionCodeDescription

The distributionCodeDescription object class is used to define a directory entry that represents a registered Distribution Code in the directory and describes its meaning. See ACP 123 for specification of distribution codes. The distribution code is held in the commonName attribute. Table B-24 shows the composition of the distributionCodeDescription object class. This object class is the base class for Distribution Code Description type directory entries.

Table B-24
distributionCodeDescription Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o

k. dSSCSPLA

The dSSCSPLA object class is used to represent an Intelligence Community (IC) Plain Language Address (PLA) organization that, in the directory, is named using the plaNameACP127 attribute. B-25 shows the composition of the dSSCSPLA object class. This object class is the base class for DSSCS PLA type directory entries.

Table B-25
dSSCSPLA Object Class

Attribute	m/o
ACP 133: adminConversion	o
ACP 133: associatedOrganization	o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: rI	m
ACP 133: serviceOrAgency*	o
ACP 133: sigad	o
ACP 133: usdConversion	o

* from plaACP127 (superclass); see paragraph 7 in this annex

l. messagingGateway

The messagingGateway object class is used to store information about an application entity which serves as an application layer gateway between two mail systems. When a gateway performs translation services, a messagingGateway object provides a mechanism to address these translation services directly. Table B-26 shows the composition of the messagingGateway object class. This object class is the base class for Messaging Gateway Ed. A type directory entries.

Table B-26
messagingGateway Object Class

Attribute	m/o
ACP 133: administrator	o
ACP 133: aigsExpanded	o
X.520: commonName*	m
X.520: description*	o
ACP 133: gatewayType	o
ACP 133: ghpType	o
RFC 1274: host	o
X.520: localityName*	o
ACP 133: mailDomains	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length*	o
X.402: mhs-message-store-dn	o
X.402: mhs-or-addresses	o
X.402: mhs-or-addresses-with-capabilities	o
X.402: mhs-unacceptable-eits	o
ACP 133: onSupported	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner*	o
ACP 133: plaNameACP127	o
X.520: presentationAddress*	m
X.520: protocolInformation*	o
ACP 133: rIIInfo	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from mhs-message-transfer-agent (superclass)

m. mLA

(1) The mLA object class is used to represent an application entity that performs the functions of a MLA. This object class is a subclass of applicationEntity and strongAuthenticationUser. Table B-27 shows the composition of the mLA object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-27
mLA Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.509: supportedAlgorithms	o
X.520: supportedApplicationContext*	o
X.509: userCertificate**	m

* from applicationEntity (superclass)

** from strongAuthenticationUser (superclass)

n. mAgent

The mAgent object class is used to represent an application entity that performs the functions of a MLA. This object class is a subclass of applicationEntity and pkiUser. Table B-28 shows the composition of the mAgent object class. This object class is the base class for MLA Ed. A type directory entries.

Table B-28
mAgent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.509: supportedAlgorithms	o
X.520: supportedApplicationContext*	o
X.509: userCertificate**	o

* from applicationEntity (superclass)

** from pkiUser (superclass)

o. network

The network structural object class is used to define directory entries representing interconnected communications networks. A Network entry can have subordinate entries that define the access and instructions for reaching other networks. Table B-29 shows the composition of the network object class. This object class is the base class for Network type directory entries. Note that Edition B of this ACP replaces the network object class (which may be removed from this ACP in future editions) with the aCPNetworkEdB object class.

Table B-29
network Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
ACP 133: networkSchema	o
ACP 133: operationName	o
X.520: seeAlso	o

p. networkInstructions

The networkInstructions structural object class is used to define a directory entry that provides the description of how to reach the subject network from another network. Table B-30 shows the composition of the networkInstructions object class. This object class is the base class for Network Instructions type directory entries. Note that Edition B of this ACP replaces the networkInstructions object class (which may be removed from this ACP in future editions) with the aCPNetworkInstructionsEdB object class.

Table B-30
networkInstructions Object Class

Attribute	m/o
ACP 133: accessCodes	o
ACP 133: accessSchema	o
X.520: commonName	m
X.520: description	o
ACP 133: networkDN	o

q. orgACP127

The orgACP127 object class is used to define the entry for a single ACP 127/JANAP 128 messaging user. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-31 shows the composition of the orgACP127 object class. This object class is the base class for Organizational PLA type directory entries.

Table B-31
orgACP127 Object Class

Attribute	m/o
ACP 133: accountingCode	o
ACP 133: associatedOrganization	o
ACP 133: community*	o
X.520: countryName	o
ACP 133: dualRoute	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: longTitle	o
ACP 133: minimize	o
ACP 133: minimizeOverride	o
ACP 133: nameClassification	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: rI	o
ACP 133: rInfo	o
ACP 133: section	o
ACP 133: serviceOrAgency*	o
X.520: stateOrProvinceName	o
ACP 133: tARE	o

* from plaACP127 (superclass); see paragraph 7 in this annex

r. plaCollectiveACP127

The plaCollectiveACP127 object class is used to define the entry for an ACP 127/JANAP 128 Address Indicator Group (AIG) distribution list or Type distribution list. This

object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-32 shows the composition of the plaCollectiveACP127 object class. This object class is the base class for PLA Collective type directory entries.

Table B-32
plaCollectiveACP127 Object Class

Attribute	m/o
ACP 133: actionAddressees	o
ACP 133: allowableOriginators	o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
X.520: description	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: infoAddressees	o
ACP 133: lastRecapDate	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

s. releaseAuthorityPerson

(1) The releaseAuthorityPerson object class is used to define the entry for a role of release authority who releases organizational messages on behalf of an organization. Whereas organizations originate their organizational messages, it is the job of the release authority to sign the messages. Release authorities do not send individual messages and do not receive messages. Entries for release authorities are subordinate to the entry for the organizationalUnit (that is a messaging user) in the DIT. Table B-33 shows the composition of the releaseAuthorityPerson object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-33
releaseAuthorityPerson Object Class

Attribute	m/o
X.509: attributeCertificate*	o
ACP 133: releaseAuthorityName	m
X.509: supportedAlgorithms*	o
X.509: userCertificate*	m

* from secure-user (superclass); see paragraph 7 in this annex

t. releaseAuthorityPersonA

The releaseAuthorityPersonA object class is used to define the entry for a role of release authority who releases organizational messages on behalf of an organization. Whereas organizations originate their organizational messages, it is the job of the release authority to sign the messages. Release authorities do not send individual messages and do not receive messages. Entries for release authorities are subordinate to the entry for the organizationalUnit (that is a messaging user) in the DIT. Table B-34 shows the composition of the releaseAuthorityPersonA object class. This object class is the base class for Release Authority Person Ed. A type directory entries.

Table B-34
releaseAuthorityPersonA Object Class

Attribute	m/o
X.509: attributeCertificate*	o
ACP 133: releaseAuthorityName	m
X.509: supportedAlgorithms*	o
X.509: userCertificate*	o

* from securePkiUser (superclass); see paragraph 7 in this annex.

u. routingIndicator

The routingIndicator object class is used to define an entry for a RI and is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-35 shows the composition of the routingIndicator object class. This object class is the base class for Routing Indicator Ed. B type directory entries.

Table B-35
routingIndicator Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
ACP 133: lmf	o
X.402: mhs-maximum-content-length	o
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: rI	m
ACP 133: rIClassification	o
ACP 133: sHD	o
ACP 133: tCC	o
ACP 133: transferStation	o
ACP 133: tRC	o

* from plaData (superclass); see paragraph 7 in this annex

v. sigintPLA

The sigintPLA object class is used to represent sensitive Signal Intelligence PLAs. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-36 shows the composition of the sigintPLA object class. This object class is the base class for Signal Intelligence PLA type directory entries.

Table B-36
sigintPLA Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: rI	o
ACP 133: shortTitle	o
ACP 133: sigad	m

* from plaData (superclass); see paragraph 7 in this annex

w. sIPLA

The sIPLA object class is used to define the entry for a single Special Intelligence (SI) messaging user. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-37 shows the composition of the sIPLA object class. This object class is the base class for Special Intelligence PLA type directory entries.

Table B-37
sIPLA Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: longTitle	m
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: rI	o
ACP 133: shortTitle	o
ACP 133: sigad	o

* from plaData (superclass); see paragraph 7 in this annex

x. spotPLA

The spotPLA object class is used to define an entry for a special products distribution list. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-38 shows the composition of the spotPLA object class. This object class is the base class for SPOT PLA type directory entries.

Table B-38
spotPLA Object Class

Attribute	m/o
ACP 133: actionAddressees	o
ACP 133: additionalAddressees	o
ACP 133: additionalSecondPartyAddressees	o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.402: mhs-dl-submit-permissions	o
ACP 133: remarks	o
ACP 133: secondPartyAddressees	o
ACP 133: spot	m

* from plaData (superclass); see paragraph 7 in this annex

y. taskForceACP127

The taskForceACP127 object class is used to define a directory entry for an ACP 127/JANAP 128 task force distribution list. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-39 shows the composition of the taskForceACP127 object class. This object class is the base class for Task Force PLA type directory entries.

Table B-39
taskForceACP127 Object Class

Attribute	m/o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: lastRecapDate	m
ACP 133: nationality*	o
ACP 133: plaAddressees	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	m
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

z. tenantACP127

The tenantACP127 object class is used to define a directory entry that represents a tenant PLA. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP, and contains the reference to the host PLA for this tenant. Table B-40 shows the composition of the tenantACP127 object class. This object class is the base class for Tenant PLA type directory entries.

Table B-40
tenantACP127 Object Class

Attribute	m/o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: hostOrgACP127	m
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o
ACP 133: tARE	o

* from plaACP127 (superclass); see paragraph 7 in this annex

6. Name Forms and DIT Structural Rules

a. The RDN of each Allied Directory entry is the distinguished value of the naming attribute(s) specified by the Name Form for the structural object class on which the directory entry is based. Although all of the directory standard name forms shall be supported for the Allied Directory System, the standard name forms used in ACP 133 entries are shown in Table B-41. As summarized in Table B-41, the Allied Directory System employs directory standard name forms as well as name forms specified in this annex.

b. Each nation will construct its own structure rules.

Table B-41
Name Forms

Structural Object Class	Naming Attribute	Name Form
aCPNetworkEdB	commonName	aCPNetworkEdBNameForm
aCPNetworkInstructionsEdB	commonName	aCPNetworkInstrEdBNameForm
addressList	commonName	addressListNameForm
aliasCommonName	commonName	aliasCNNameForm
aliasOrganizationalUnit	organizationalUnitName	aliasOONameForm
altSpellingACP127	plaNameACP127	alternateSpellingPLANameForm
applicationEntity	commonName and, optionally, dnQualifier	aENNameForm
applicationProcess	commonName	applProcessNameForm (X.521)
cadACP127	plaNameACP127	cadPLANameForm

Structural Object Class	Naming Attribute	Name Form
country	countryName	countryNameForm (X.521)
cRLDistributionPoint	commonName	cRLDistPtNameForm (X.521)
device	commonName	deviceNameForm (X.521)
distributionCodeDescription	commonName	distributionCodeDescriptionNameForm
dSA	commonName	dSANameForm (X.521)
dSSCSPLA	plaNameACP127	dSSCSPLANameForm
groupOfNames	commonName	gONNameForm (X.521)
locality	localityName or stateOrProvinceName	locNameForm (X.521) or sOPNameForm (X.521)
messagingGateway	commonName	messagingGatewayNameForm
mhs-distribution-list	commonName	mhs-dLNameForm
mhs-message-store	commonName	mSNameForm
mhs-message-transfer-agent	commonName	mTANameForm
mhs-user-agent	commonName	mUANameForm
mLA	commonName	mLANameForm
mLAgent	commonName	mLAgentNameForm
network	commonName	networkNameForm
networkInstructions	commonName	networkInstructionsNameForm
organization	organizationName and, optionally, dnQualifier	organizationNameForm
organizationalPerson	commonName and, optionally, dnQualifier or organizationalUnitName	qualifiedOrgPersonNameForm
orgACP127	plaNameACP127	organizationalPLANameForm
organizationalRole	commonName and, optionally, dnQualifier	orgRNameForm
organizationalUnit	organizationalUnitName and, optionally, dnQualifier	orgUNameForm
plaCollectiveACP127	plaNameACP127	plaCollectiveNameForm
releaseAuthorityPerson	releaseAuthorityName	releaseAuthorityPersonNameForm
releaseAuthorityPersonA	releaseAuthorityName	releaseAuthorityPersonANameForm
routingIndicator	rI	routingIndicatorNameForm
sigintPLA	sigad	sigintPLANameForm
sIPLA	longTitle	sIPLANameForm
spotPLA	spot	spotPLANameForm
taskForceACP127	plaNameACP127	taskForcePLANameForm
tenantACP127	plaNameACP127	tenantPLANameForm

SECTION III

COMMON AUXILIARY OBJECT CLASSES AND ATTRIBUTES

7. Common Auxiliary Object Classes

The Allied Directory System Common Content includes auxiliary object classes defined in the directory and MHS standards and in this ACP. The Common Content uses the certificationAuthority-V2 and pkiCA auxiliary object classes, specified in X.521 and X.509 and DAM 1 for the 1997 versions, as auxiliary object classes of Allied Directory Entries. The auxiliary object of mhs-user defined in X.402 is also used in the Common Content.

a. Superclasses

Each of these standard classes is used in the Common Content as a superclass in the definition of a standard auxiliary object class, as described below, or of an auxiliary object class defined in this ACP:

- certificationAuthority (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- pkiUser
- strongAuthenticationUser (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

b. Other Standard Auxiliary Object Classes

The standard auxiliary object classes that are included in the Common Content, but are not used in meeting Allied Directory requirements are:

- deltaCRL
- userSecurityInformation

c. ACP 133-specific Auxiliary Object Classes

The auxiliary object classes for Common Content, specified in this annex, are:

- distributionCodesHandled
- otherContactInformation
- plaACP127
- plaData

- plaUser
- secure-user
- securePkiUser
- ukms

d. certificationAuthority-V2

(1) The certificationAuthority-V2 object class is used in defining directory entries for objects which act as CAs, as defined in ITU-T Rec. X.521 | ISO/IEC 9594-7. Table B-42 shows the composition of the certificationAuthority-V2 object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-42
certificationAuthority-V2 Object Class

Attribute	m/o
X.509: authorityRevocationList*	m
X.509: cACertificate*	m
X.509: certificateRevocationList*	m
X.509: crossCertificatePair*	o
X.509: deltaRevocationList	o

* from certificationAuthority (superclass)

e. deltaCRL

The deltaCRL object class is not used for Allied Directory entries, but is described in X.521 (1997) DAM 1.

f. distributionCodesHandled

The distributionCodesHandled object class provides for identifying the distribution codes (e.g., Subject Indicator Codes (SIC) as defined in NATO Subject Indicator System - publication 3 (NASIS APP-3) and supplements) which are handled, either for action or information, by the object (e.g., organizational role, organizational person, or organizational unit) represented by the directory entry in which this auxiliary is included. Table B-43 shows the composition of the distributionCodesHandled object class.

Table B-43
distributionCodesHandled Object Class

Attribute	m/o
ACP 133: distributionCodeAction	o
ACP 133: distributionCodeInfo	o

g. mhs-user

(1) The mhs-user object class is used in defining directory entries representing MHS users. The attributes in an entry identify the MHS user's OR-address and, to the extent that the relevant attributes are present, identify the maximum content length, content types, and EITs that can be handled by the user; its MS; and its preferred delivery methods. Table B-44 shows the composition of the mhs-user object class.

Table B-44
mhs-user Object Class

Attribute	m/o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-message-store-dn	o
X.402: mhs-or-addresses	m
X.402: mhs-or-addresses-with-capabilities	o
X.402: mhs-unacceptable-eits	o

(2) If the MHS user has multiple OR-addresses, which have differing deliverability capabilities, then the attributes mhs-deliverable-content-types, mhs-deliverable-eits, and mhs-undeliverable-eits should represent the union of these deliverability capabilities; the attribute mhs-maximum-content-length should contain the largest of the values of this attribute. The capability available at each OR-address can then be determined, when required, from the attribute mhs-or-addresses-with-capabilities.

h. otherContactInformation

The otherContactInformation object class provides for additional telephone, location, and mailbox information in directory entries. Table B-45 shows the composition of the otherContactInformation object class.

Table B-45
otherContactInformation Object Class

Attribute	m/o
ACP 133: aCPMobileTelephoneNumber	o
ACP 133: aCPPagerTelephoneNumber	o
ACP 133: aCPPREFERREDDELIVERY	o
ACP 133: mailDomains	o
ACP 133: militaryFacsimileNumber	o
ACP 133: militaryTelephoneNumber	o
ACP 133: proprietaryMailboxes	o
RFC 1274: roomNumber	o
ACP 133: secureFacsimileNumber	o
ACP 133: secureTelephoneNumber	o

i. pkiCA

The pkiCA object class, defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 DAM 1, is used in defining directory entries for Certification Authorities. Table B-46 shows the composition of the pkiCA object class.

Table B-46
pkiCA Object Class

Attribute	m/o
X.509: authorityRevocationList	o
X.509: cACertificate	o
X.509: certificateRevocationList	o
X.509: crossCertificatePair	o

j. pkiUser

The pkiUser object class is used in defining directory entries for objects that include user certificates, as defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 DAM 1. Table B-47 shows the composition of the pkiUser object class.

Table B-47
pkUser Object Class

Attribute	m/o
X.509: userCertificate	o

k. plaACP127

The plaACP127 object class provides for the general PLA attributes common to general service (GENSER) PLA entries, all of which inherit this class. Table B-48 shows the composition of the plaACP127 object class. This object class is the superclass of the base class for Alternate Spelling PLA, CAD PLA, DSSCS PLA, Organizational PLA, PLA Collective, Task Force PLA, and Tenant PLA type directory entries.

Table B-48
plaACP127 Object Class

Attribute	m/o
ACP 133: community	o
ACP 133: effectiveDate	o
ACP 133: expirationDate	o
ACP 133: nationality	o
ACP 133: plaNameACP127	m
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: serviceOrAgency	o

l. plaData

The plaData object class contains attributes common to SI PLAs. Table B-49 shows the composition of the plaData object class. This object class is the superclass of the base class for Routing Indicator, Signal Intelligence PLA, Special Intelligence PLA, and SPOT PLA type directory entries.

Table B-49
plaData Object Class

Attribute	m/o
ACP 133: community	o
X.520: description	o
ACP 133: effectiveDate	o
ACP 133: expirationDate	o

m. plaUser

The plaUser object class contains the name of a PLA's directory entry and, optionally, RI for addressing that PLA. Table B-50 shows the composition of the plaUser object class.

Table B-50
plaUser Object Class

Attribute	m/o
ACP 133: plaNameACP127	m
ACP 133: rInfo	o

n. secure-user

(1) The secure-user object class is used in defining directory entries that include credentials for ACP 123 users. It is a subclass of the strongAuthenticationUser object class, defined in X.521, which provides for a user certificate. Table B-51 shows the composition of the secure-user object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-51
secure-user Object Class

Attribute	m/o
X.509: attributeCertificate	o
X.509: supportedAlgorithms	o
X.509: userCertificate*	m

* from strongAuthenticationUser (superclass)

o. securePkiUser

The securePkiUser object class is used in defining directory entries that include credentials for ACP 123 users. It is a subclass of the pkiUser object class, defined in X.509 DAM 1, which provides for a user certificate. Table B-52 shows the composition of the securePkiUser object class.

Table B-52
securePkiUser Object Class

Attribute	m/o
X.509: attributeCertificate	o
X.509: supportedAlgorithms	o
X.509: userCertificate*	o

* from pkiUser (superclass)

p. ukms

The ukms object class contains the monthly values of user keying material (UKM) used in the construction of selected CCEB symmetric confidentiality algorithms. Table B-53 shows the composition of the ukms object class.

Table B-53
ukms Object Class

Attribute	m/o
ACP 133: janUKMs	o
ACP 133: febUKMs	o
ACP 133: marUKMs	o
ACP 133: aprUKMs	o
ACP 133: mayUKMs	o
ACP 133: junUKMs	o
ACP 133: julUKMs	o
ACP 133: augUKMs	o
ACP 133: sepUKMs	o
ACP 133: octUKMs	o
ACP 133: novUKMs	o
ACP 133: decUKMs	o

q. userSecurityInformation

The userSecurityInformation object class is not used for Allied Directory entries, but is described in X.521 (1997).

8. Attributes in Common Content Object Classes

This paragraph lists the attributes that are included in the structural and auxiliary object classes in the Common Content. Paragraph 9 gives the attributes in the Common Content that can be added by content rules. The attributes are defined in the Directory and MHS standards, in RFC 1274, and in this ACP. All of the attributes used in the Common Content are described in Section IX of this annex.

a. Directory Standard Attributes

The attributes in the Common Content that are defined in the directory standards and are used to meet Allied Directory requirements are:

- aliasedEntryName
- attributeCertificate
- authorityRevocationList
- businessCategory
- caCertificate
- certificateRevocationList
- commonName
- countryName
- postalAddress
- postalCode
- postOfficeBox
- preferredDeliveryMethod
- presentationAddress
- protocolInformation
- registeredAddress
- roleOccupant

- crossCertificatePair
- deltaRevocationList
- description
- destinationIndicator
- distinguishedName
- facsimileTelephoneNumber
- internationalISDNNumber
- knowledgeInformation
- localityName
- member
- name
- organizationalUnitName
- organizationName
- owner
- physicalDeliveryOfficeName
- searchGuide
- seeAlso
- serialNumber
- stateOrProvinceName
- streetAddress
- supportedAlgorithms
- supportedApplicationContext
- surname
- telephoneNumber
- teletexTerminalIdentifier
- telexNumber
- title
- userCertificate
- userPassword
- x121Address

b. MHS Standard Attributes

The attributes in the Common Content that are defined in the MHS standards are:

- mhs-acceptable-eits
- mhs-deliverable-classes
- mhs-deliverable-content-types
- mhs-dl-archive-service
- mhs-dl-members
- mhs-dl-policy
- mhs-dl-related-lists
- mhs-dl-submit-permissions
- mhs-dl-subscription-service
- mhs-exclusively-acceptable-eits
- mhs-maximum-content-length
- mhs-message-store-dn
- mhs-or-addresses
- mhs-or-addresses-with-capabilities
- mhs-supported-attributes
- mhs-supported-automatic-actions
- mhs-supported-content-types
- mhs-supported-matching-rules
- mhs-unacceptable-eits

c. RFC 1274-defined Attributes

The attributes in the Common Content that are defined in RFC 1274 are:

- buildingName
- host
- rfc822Mailbox
- roomNumber

d. ACP 133-defined Attributes

The attributes in the Common Content that are defined in this ACP are:

- accessCodes
- accessSchema
- aCPMobileTelephoneNumber
- aCPNetwAccessSchemaEdB
- aCPNetworkSchemaEdB
- aCPPagerTelephoneNumber
- aCPPreferredDelivery
- accountingCode
- aCPTelephoneFaxNumber
- actionAddressees
- additionalAddressees
- additionalSecondPartyAddressees
- adminConversion
- administrator
- aigsExpanded
- aLExemptedAddressProcessor
- aliasPointer
- alid
- allowableOriginators
- aLReceiptPolicy
- alternateRecipient
- aLType
- aprUKMs
- associatedAL
- associatedOrganization
- associatedPLA
- augUKMs
- cognizantAuthority
- community
- copyMember
- decUKMs
- deployed
- distributionCodeAction
- distributionCodeInfo
- dualRoute
- effectiveDate
- entryClassification
- expirationDate
- febUKMs
- garrison
- listPointer
- lmf
- longTitle
- mailDomains
- marUKMs
- mayUKMs
- militaryFacsimileNumber
- militaryTelephoneNumber
- minimize
- minimizeOverride
- nameClassification
- nationality
- networkDN
- networkSchema
- novUKMs
- octUKMs
- onSupported
- operationName
- plaAddressees
- plaNameACP127
- plaReplace
- plasServed
- positionNumber
- primarySpellingACP127
- proprietaryMailboxes
- publish
- rank
- recapDueDate
- releaseAuthorityName
- remarks
- rI
- rIClassification
- rIInfo
- secondPartyAddressees
- section
- secureFacsimileNumber
- secureTelephoneNumber
- sepUKMs
- serviceNumber
- serviceOrAgency

- gatewayType
- ghpType
- guard
- hostOrgACP127
- infoAddressees
- janUKMs
- julUKMs
- junUKMs
- lastRecapDate
- sHD
- shortTitle
- sigad
- spot
- tARE
- tCC
- transferStation
- tRC
- usdConversion

e. Other Standard Attributes

There are several other standard attributes that are included in the Common Content, but are not used to meet Allied Directory requirements. The other standard attributes are:

- enhancedSearchGuide
- generationQualifier
- givenName
- houseIdentifier
- initials
- uniqueIdentifier
- uniqueMember

9. Attributes Added by Content Rules

The Common Content uses the dnQualifier and the businessCategory attributes from X.520 as additional attributes. The buildingName and rfc822Mailbox attributes from RFC 1274 are additional attributes in the Common Content. The additional attributes for Common Content, specified in this annex, are:

- aCPLegacyFormat
- aliasPointer
- alternateRecipient
- associatedAL
- associatedOrganization

- associatedPLA
- effectiveDate
- expirationDate
- guard
- listPointer
- nationality
- plasServed
- positionNumber
- rank
- remarks
- serviceNumber
- tCCG

10. Collective Attributes

a. These standard attributes from X.520 may be included in a collectiveAttributeSubentry:

- collectiveFacsimileTelephoneNumber
- collectiveInternationalISDNNumber
- collectiveLocalityName
- collectiveOrganizationalUnitName
- collectiveOrganizationName
- collectivePhysicalDeliveryOfficeName
- collectivePostalAddress
- collectivePostalCode
- collectivePostOfficeBox
- collectiveStateOrProvinceName

- collectiveStreetAddress
 - collectiveTelephoneNumber
 - collectiveTeletexTerminalIdentifier
 - collectiveTelexNumber
- b. These attributes, defined in this annex, may be included in a collectiveAttributeSubentry:
- collective-mhs-or-addresses
 - collectiveMilitaryFacsimileNumber
 - collectiveMilitaryTelephoneNumber
 - collectiveNationality
 - collectiveSecureFacsimileNumber
 - collectiveSecureTelephoneNumber
- c. Since collective attributes are defined as subtypes of user attributes, they are returned whenever a query is made for the supertype. Thus, the use of collective attributes allows a single point of administration for certain attributes where many entries have the same value. DSAs shall support collective attributes; whether the facility is used is a national matter. Collective attributes that apply to entries which are shadowed shall be passed with the shadowed information.

SECTION IV

APPLYING CONTENT RULES IN THE COMMON CONTENT

11. Common Content

- a. The Allied Directory System Common Content is a set of structural and auxiliary object classes and additional attributes that are combined to form a variety of types of directory entries. Content rules defined for any DIT subtree schema dictate the allowed combinations. Suggested combinations are shown in Table B-54. The combinations marked with “•” represent the ACP 133 Edition B example content rules. The combinations marked with “o” represent combinations in the original ACP 133 that are not included in the Edition B content rules. The types of directory entries that are in the Allied Directory System are defined in paragraph 12 of this section.
- b. All of the structural object classes, auxiliary object classes, and additional attributes in the Common Content shall be supported.

c. The structural object classes are shown across the top of the table forming the columns of the table. The name of each structural object class is prefixed by the source of its definition. For example, aliasCommonName is defined in ACP 133, and country is defined in X.521.

d. The auxiliary object classes that may be used in a content rule are shown down the left-hand side. The attributes that may also be included in a content rule for a directory entry based on the structural object class are also shown down the left-hand side. Each auxiliary object class and additional attribute is prefixed by the source of its definition.

e. An example of how to read the chart is as follows: the content rule for the structural object class organizationalUnit (the "X.521: organizationalUnit" column) shows that entries based on this class may also belong to the auxiliary object classes: distributionCodesHandled, mhs-user, otherContactInformation, plaUser, securePkiUser, and ukms. Also, the entry may include the aCPLegacyFormat, aliasPointer, alternateRecipient, associatedPLA, deployed, dnQualifier, effectiveDate, expirationDate, garrison, guard, listPointer, nationality, and rfc822Mailbox attributes.

f. In paragraph 205, the suggested content rules are defined using the formal ASN.1 template defined in X.501. National schemas may change or expand these content rules, if necessary, to include nationally specific auxiliary object classes and additional attributes. Attributes may be made mandatory or optional. Also, attributes which are optional in the structural or auxiliary object classes may be precluded in a content rule.

g. Content rules control which attributes may or may not appear in an entry. When, for example, a directory entry for a suborganization is being added to the Allied Directory System DIB, the organizationalUnit structural object class is used. The value of the entry's objectClass Attribute is set to indicate the entry is of this class. The content rule for organizationalUnit then determines what other auxiliary classes and attributes may be added to increase the attribute types that are allowed or required in the entry. When an auxiliary object class allowed by the content rule is added to the directory entry, the object identifier for the auxiliary object class is also included in the objectClass attribute in the entry. Thus, if the suborganization is also a messaging user, the objectClass attribute in the entry would include at least the two object identifier values: organizationalUnit and mhs-user.

Table B-54
Common Content

Structural Object Classes	Auxiliary Object Classes	
	Auxiliary Classes	Object Classes
ACP 133: ACPPNetworKEFDB	X.521: certificationAuthority-V2	
ACP 133: ACPPNetworKInstrumentsEDB	ACP 133: distributionCodesHandled	
ACP 133: addressList	X.402: mhs-user	
ACP 133: aliasCommonName	ACP 133: otherContactInformation	
ACP 133: applicationProcess	X.509: pkICA	
X.521: countY	ACP 133: pkACPI27	
X.521: CRLDistributionPoint	ACP 133: plaData	
X.521: device	ACP 133: plUser	
ACP 133: distributionCodeDescription	ACP 133: secure-user	
X.521: locality	X.509: deltaCRL	
ACP 133: messagingGateway	X.521: userSecurityInformation	
X.521: organization		
ACP 133: network		
ACP 133: netwerkinstuctions		
X.521: organizationUnit		
X.402: mhs-user-agent		
X.402: mhs-message-store		
X.402: mhs-distribution-list		
ACP 133: messageStore		
X.402: mhs-message-store		
X.402: mhs-messagetransfer-agent		
X.402: mhs-user-agent		
ACP 133: mLAgent		
ACP 133: network		
ACP 133: netwerkinstuctions		
X.521: organizationUnit		
X.521: releaseAuthorityPerson		
ACP 133: releaseAuthorityPersonA		
ACP 133: releaseAuthorityPersonA		
ACP 133: orgACPI27		
ACP 133: placeEffectiveACPI27		
ACP 133: routingIndicator		
ACP 133: signPLA		
ACP 133: spotPLA		
ACP 133: tenantACPI27		
ACP 133: taskForceACPI27		
ACP 133: siPLA		
ACP 133: signPLA		
ACP 133: readACPI27		
ACP 133: dSSCPLA		
ACP 133: orgACPI27		
ACP 133: orgACPI27		
X.521: residentialPerson		

- denotes a combination as defined in Annex B, paragraph 11
- denotes a combination as defined in the original ACP 133, but not in later editions

* Other Standard Structural Object Class

Table B-54 (cont.)
Common Content

- denotes a combination as defined in Annex B, paragraph 11

\bullet denotes a combination as defined in the original ACP 133, but not in later editions

* Other Standard Structural Object Class

12. Directory Entries

The Allied Directory System contains the following types of directory entries.

a. Address List Ed. A

(1) An Address List Ed. A directory entry provides for a group of users that are named and addressed as a group for messaging purposes. This directory entry should include especially the list address, its security materials, and its members.

(2) This directory entry uses a content rule based on the structural object class, addressList, which is defined in Section XII of this annex. An example of such a content rule is the addressListRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- plaUser object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

b. Address List Alias

(1) An Address List Alias directory entry provides for an alternative means of naming and referring to an address list.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in this ACP (Section XII of this annex).

(3) The aliasedEntryName attribute value is the name of the Address List Ed. A directory entry.

c. Alternate Spelling PLA

(1) An Alternate Spelling PLA directory entry provides for an alternate spelling of a PLA; it contains a reference to the PLA for which it is an alternate spelling.

(2) This directory entry is based on the structural object class, altSpellingACP127, which is defined in Section XII of this annex.

d. Application Entity Ed. A

(1) An Application Entity Ed. A directory entry provides a means of referring to those aspects of an application process that are pertinent to communications, such as Presentation Service Access Point address. It may also store certificates used for strong authentication. This type of directory entry is used for applications in an Allied communications network.

(2) This directory entry uses a content rule based on the structural object class, applicationEntity, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPApplicationEntityRuleEdA in this annex. The directory object may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in this ACP, Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in this ACP, Section XII of this annex
- aliasPointer attribute, defined in this ACP, Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in this ACP, Section XII of this annex
- expirationDate attribute, defined in this ACP, Section XII of this annex

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

e. Application Process

(1) An Application Process directory entry provides for representing an application process. An application process is an element within a computer system which performs the information processing for a particular application.

(2) This directory entry is based on the structural object class, applicationProcess, which is defined in ITU-T Rec. X.521.

f. CAD PLA

(1) A CAD PLA directory entry provides for naming and referring to an ACP 127/JANAP 128 distribution list. CADs are medium-to-large distribution lists used to address homogeneous activities and which are centrally defined and programmed into AUTODIN switching centers.

(2) This directory entry is based on the structural object class, cadACP127, which is defined in Section XII of this annex.

g. Certification Authority Ed. B

(1) A Certification Authority Ed. B directory entry provides for naming and referring to a CA. It provides the security information of a CA for certificate management.

(2) The naming attributes distinguished values for naming shall comply with paragraph 305.

(3) This directory entry uses any one of the content rules based on the structural object classes: applicationEntity, organization, organizationalUnit, and organizationalRole, which are defined in ITU-T Rec. X.521. Examples of such content rules are the aCPApplicationEntityRuleEdA, aCPOrganizationRuleEdB, aCPOrganizationalUnitRuleEdB, and aCPOrganizationalRoleRuleEdB in this annex. Certification Authority Ed. B directory entries are different from other types of entries in that the pkiCA auxiliary object class, defined in ITU-T Rec. X.521 DAM 1, is included. A Certification Authority Ed. B directory entry may also include the other auxiliary object classes and additional attributes that are permitted by the content rule which governs the entry.

h. Country

(1) A Country directory entry is generally directly under the root of the DIT and provides the first level of the DIT for each and every Ally providing and using the Allied Directory services.

(2) This directory entry is based on the structural object class, country, which is defined in ITU-T Rec. X.521.

i. CRL Distribution Point

(1) A CRL Distribution Point directory entry provides for holding a CRL that is a subset of the complete CRL issued by one CA or that is a combination of CRLs issued by different CAs.

(2) This directory entry uses a content rule based on the structural object class, cRLDistributionPoint, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPCRLDistributionPointRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

j. Device Ed. A

(1) A Device Ed. A directory entry represents a physical unit which can communicate, such as a modem, printer, etc., with optional authentication capability.

(2) This directory entry uses a content rule based on the structural object class, device, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPDeviceRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

k. Distribution Code Description

(1) A Distribution Code Description directory entry represents a registered Distribution Code in the directory and describes its meaning. The distribution code is the value of the RDN of the directory entry.

(2) This directory entry is based on the structural object class, distributionCodeDescription, which is defined in Section XII of this annex. An example of such a content rule is the distributionCodeDescriptionRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

I. DSA Ed. A

(1) A DSA Ed. A directory entry provides the addressing and security information for a DSA. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, dSA, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPDSARuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

m. DSSCS PLA

(1) A DSSCS PLA directory entry provides for a single IC legacy messaging organization.

(2) This directory entry is based on the structural object class, dSSCSPLA, which is defined in Section XII of this annex.

n. Group of Names

(1) A Group of Names directory entry defines an unordered set of DNs which represent individual directory entries or other groups of names. The membership of a group is static, i.e., it is explicitly modified by administrative action, rather than dynamically determined each time reference is made to the group. Group of Names directory entries are useful in constructing access control lists.

(2) This directory entry uses a content rule based on the structural object class, groupOfNames, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPGroupOfNamesRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

o. Group of Unique Names

A Group of Unique Names directory entry is based on the structural object class, groupOfUniqueNames, but is not used to meet Allied Directory requirements.

p. Locality

(1) A Locality directory entry provides for accessing entries that are referred to by a locality-named subtree in the DIT.

(2) This directory entry uses a content rule based on the structural object class, locality, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPLocalityRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

q. Messaging Gateway Ed. A

(1) A Messaging Gateway Ed. A directory entry stores information about an Allied MMHS messaging gateway component that translates message content types, which may include RFC 822, ACP 127/JANAP 128, P22, P2, P772, and ACP 120. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, messagingGateway, which is defined in Section XII of this annex. An example of such a content rule is the messagingGatewayRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- plasServed attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

r. Messaging Organizational Unit Alias

(1) An Messaging Organizational Unit Alias directory entry provides for an alternative means of naming and referring to a suborganization as a messaging user.

(2) This directory entry uses a content rule based on the structural object class, aliasOrganizationalUnit, which is defined in Section XII of this annex. An example of such a content rule is the aliasOrganizationalUnitRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Unit directory entry that includes the mhs-user auxiliary object class.

s. MHS Distribution List

(1) An MHS Distribution List directory entry represents an AL that is expanded by the MHS. The attributes in this type of entry identify the common name, submit permissions, and OR-addresses of the address list and, to the extent that the relevant attributes are present, describe the address list, identify its organization, organizational units, and owner; cite related objects; identify its maximum content length, deliverable content types, and acceptable, exclusively acceptable, and unacceptable EITs; and identify the expansion policy, subscription addresses, archive addresses, related lists, and members of the AL.

(2) This directory entry uses a content rule based on the structural object class, mhs-distribution-list, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-distribution-listRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

t. MHS Message Store Ed. A

(1) An MHS Message Store Ed. A directory entry stores information about an Allied MMHS MS component to describe the message store, identify its owner, and enumerate the attributes, automatic actions, matching rules, and content types the MS supports. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mhs-message-store, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-message-storeRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that the secure-user object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex

- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

u. MHS Message Transfer Agent Ed. A

(1) An MHS Message Transfer Agent Ed. A directory entry stores information about an Allied MMHS MTA component to describe the MTA and identify its owner and its deliverable content length. It may also store certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mhs-message--transfer-agent, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-message-transfer-agentRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

v. MHS User Agent

(1) An MHS User Agent directory entry stores information about an Allied MMHS UA component to identify the UA's owner; its deliverable content length, content types, and EITs; and its O/R address.

(2) This directory entry uses a content rule based on the structural object class, mhs-user-agent, defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-user-agentRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

w. MLA Ed. A

(1) An MLA (mail list agent) Ed. A directory entry stores addressing, security, and descriptive information about an Allied MMHS MLA component. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mLAgent, which is defined in Section XII of this annex. An example of such a content rule is the mLAgentRule in this annex. The directory entry may also include the additional attributes:

aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex. (Note that the mLAgent object class replaces the mLA object class, which may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

x. Network Ed. B

(1) A Network Ed. B directory entry represents a communications network that is connected to other networks that are also represented in the Allied DIB. A Network Ed. B entry can have subordinate entries that define the access to and instructions for reaching other networks.

(2) This directory entry uses a content rule based on the structural object class, aCPNetworkEdB, which is defined in Section XII of this annex. An example of such a content rule is the networkEdBRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

y. Network Instructions Ed. B

(1) A Network Instructions Ed. B directory entry provides the description of how to reach the subject network from the network represented by the superior entry. When there is a series of networks between the pair being represented, the instructions shall take into account any extra steps that are required.

(2) This directory entry uses a content rule based on the structural object class, aCPNetworkInstructionsEdB, which is defined in Section XII of this annex. An example of such a content rule is the networkInstructionsEdBRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

z. Organization Ed. B

(1) An Organization Ed. B directory entry provides the level of the DIT immediately below the Country directory object, for an Ally or for international/multinational organizations such as NATO and is used for locating the entries used in providing and using the Allied Directory services.

(2) This directory entry uses a content rule based on the structural object class, organization, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationRuleEdB in this annex. The directory entry may also include the auxiliary object class, otherContactInformation, and the additional attributes: dnQualifier, which is defined in ITU-T Rec. X.520, and aCPLegacyFormat, aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

aa. Organizational Person Ed. B

(1) An Organizational Person Ed. B directory entry stores information, representing an individual as a member of an organization and, optionally, representing that individual as a user of applications, such as electronic messaging. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, organizationalPerson, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalPersonRuleEdB in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- otherContactInformation object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- businessCategory attribute, defined in ITU-T Rec. X.520
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex

- nationality attribute, defined in Section XII of this annex
- positionNumber attribute, defined in Section XII of this annex
- rank attribute, defined in Section XII of this annex
- rfc822MailBox attribute, defined in RFC 1274
- serviceNumber attribute, defined in Section XII of this annex

bb. Organizational Person Alias

(1) An Organizational Person Alias directory entry provides for an alternative means of naming and referring to an organizational person.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Person Ed. B directory entry.

cc. Organizational PLA

(1) An Organizational PLA directory entry provides for a single ACP 127/JANAP 128 messaging organization.

(2) This directory entry is based on the structural object class, orgACP127, which is defined in Section XII of this annex.

dd. Organizational Role Ed. B

(1) An Organizational Role Ed. B directory entry stores information representing a role or function, such as, security officer, which is performed by one or more persons. The information includes whatever is needed for the role to participate as a user in applications, such as electronic messaging. It may also store certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, organizationalRole, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalRoleRuleEdB in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402

- otherContactInformation object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- businessCategory attribute, defined in ITU-T Rec. X.520
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry, see paragraph 12 g. Also, see paragraph 12 ii, Release Authority Role Ed. B.

ee. Organizational Role Alias

(1) An Organizational Role Alias directory entry provides for an alternative means of naming and referring to an organizational role.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include

the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Role Ed. B directory entry.

ff. Organizational Unit Ed. B

(1) An Organizational Unit Ed. B directory entry provides a level of the DIT immediately below the Organization Ed. B directory entry of an Ally or another Organizational Unit Ed. B directory entry. An Organizational Unit Ed. B directory entry represents a suborganization and is used for navigating to directory entries belonging to that suborganization, e.g., Organizational Role Ed. B directory entries.

(2) This directory entry uses a content rule based on the structural object class, organizationalUnit, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalUnitRuleEdB in this section. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- otherContactInformation object class, defined in Section XII of this annex
- plaUser object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- associatedPLA attribute, defined in Section XII of this annex
- buildingName attribute, defined in RFC 1274
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520

- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

gg. Organizational Unit Alias

(1) An Organizational Unit Alias directory entry provides an alternative means of naming and referring to an organizational unit.

(2) This directory entry uses a content rule based on the structural object class, aliasOrganizationalUnit, which is defined in Section XII of this annex. An example of such a content rule is the aliasOrganizationalUnitRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Unit Ed. B directory entry.

hh. PLA Collective

(1) A PLA Collective directory entry provides for an ACP 127/JANAP 128 AIG distribution list or Type distribution list. A Type collective is composed of military units of the same type such as destroyers.

(2) This directory entry is based on the structural object class, plaCollectiveACP127, which is defined in Section XII of this annex.

ii. Release Authority Person Ed. A

(1) A Release Authority Person Ed. A directory entry provides the certificate information used by a release authority to sign organizational messages and for strong authentication. The function fulfilled by a Release Authority is defined as a national matter. To validate that the object represented by the directory entry is an authorized Release Authority, the certificate must be checked.

(2) This directory entry type is used by the U.S., where messages are sent to organizations. Because organizational messages are sent to organizations, originators in other countries do not need to query the Allied Directory for a Release Authority. The ability of the originator to release organizational messages is checked by examining the certificate.

(3) This directory entry uses a content rule based on the structural object class, `releaseAuthorityPersonA`, which is defined in Section XII of this annex. An example of such a content rule is the `rAPersonRuleEdA` in this annex. The directory entry may also include the additional attributes: `effectiveDate`, and `expirationDate`, which are defined in Section XII of this annex. (Note that the `releaseAuthorityPersonA` object class replaces the `releaseAuthorityPerson` object class, which may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

jj. Release Authority Role Ed. B

(1) A Release Authority Role Ed. B directory entry provides the certificate information used by a release authority to send and receive organizational messages and for strong authentication. The function fulfilled by a Release Authority is defined as a national matter. To validate that the object represented by the directory entry is an authorized Release Authority, the certificate must be checked.

(2) The `commonName` attribute distinguished value for naming shall be “release authority,” as specified in paragraph 307. It is this naming convention that differentiates a Release Authority Role Ed. B entry from other entries that are based on the `organizationalRole` object class.

(3) This directory entry uses a content rule based on the structural object class, `organizationalRole`, which is defined in ITU-T Rec. X.521. An example of such a content rule is the `aCPOrganizationalRoleRuleEdB` in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- `distributionCodesHandled` object class, defined in Section XII of this annex
- `mhs-user` object class, defined in ITU-T Rec. X.402
- `otherContactInformation` object class, defined in Section XII of this annex
- `secure-user` object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- `securePkiUser` object class, defined in Section XII of this annex
- `ukms` object class, defined in Section XII of this annex
- `aCPLegacyFormat` attribute, defined in Section XII of this annex
- `aliasPointer` attribute, defined in Section XII of this annex

- alternateRecipient attribute, defined in Section XII of this annex
- deployed attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

kk. Residential Person

A Residential Person directory entry is based on the structural object class, groupOfUniqueNames, but is not used to meet Allied Directory requirements.

ll. Routing Indicator Ed. B

(1) A Routing Indicator Ed. B directory entry provides the description for an ACP 127/JANAP 128 RI.

(2) The directory entry uses a content rule based on the structural object class, routingIndicator, which is defined in Section XII of this annex. An example of such a content rule is the aCPRoutingIndicatorRuleEdB in this annex. The directory entry may also include the additional attributes: remarks, and tCCG, which are defined in Section XII of this annex.

mm. Signal Intelligence PLA

(1) A Signal Intelligence PLA directory entry provides for sensitive SI PLAs.

(2) This directory entry uses a content rule based on the structural object class, sigintPLA, which is defined in Section XII of this annex. An example of such a content rule is the sigintPLARule in this annex. The directory entry may also include the additional attribute: associatedOrganization, which is defined in this ACP (Section XII of this annex).

nn. Special Intelligence PLA

(1) An Special Intelligence PLA directory entry provides for a single SI messaging user of ACP 127/JANAP 128.

(2) The directory entry is based on the structural object class, siPLA, which is defined in Section XII of this annex.

oo. SPOT PLA

(1) A SPOT PLA directory entry provides for special products distribution lists used in ACP 127/JANAP 128.

(2) This directory entry uses a content rule based on the structural object class, spotPLA, which is defined in Section XII of this annex. An example of such a content rule is the spotPLARule in this annex. The directory entry may also include the additional attribute: associatedAL, which is defined in this ACP (Section XII of this annex).

pp. Task Force PLA

(1) A Task Force PLA directory entry provides the composition and description of an ACP 127/JANAP 128 task force distribution list.

(2) This directory entry is based on the structural object class, taskForceACP127, which is defined in Section XII of this annex.

qq. Tenant PLA

(1) A Tenant PLA directory entry provides the reference to the host PLA for this tenant. An example of a host is a ship and of a tenant, a Marine detachment on the ship.

(2) This directory entry is based on the structural object class, tenantACP127, which is defined in Section XII of this annex.

SECTION V

OBJECT CLASSES HIERARCHY

13. ACP 133-defined Object Classes

The relationship of the object classes, both standard and ACP-defined, included in the Common Content are shown in Figure B-1.

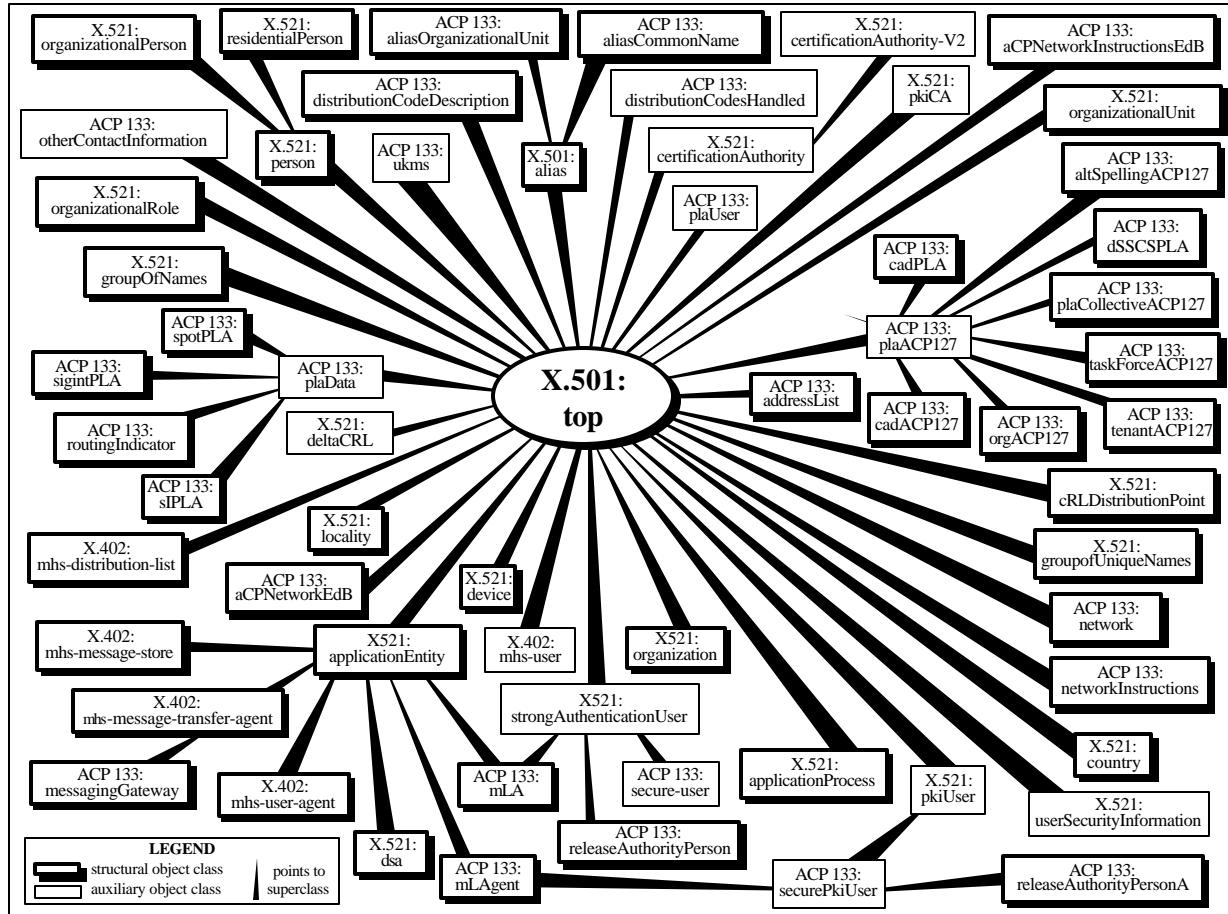


Figure B-1
Hierarchy of Common Content Object Classes

SECTION VI

ATTRIBUTE TYPES HIERARCHY

14. Attribute Subtypes

Figure B-2 shows the attributes in the Common Content that are defined as subtypes of other attributes. This indicates the subtype attributes that may be included in operations involving the parent types.

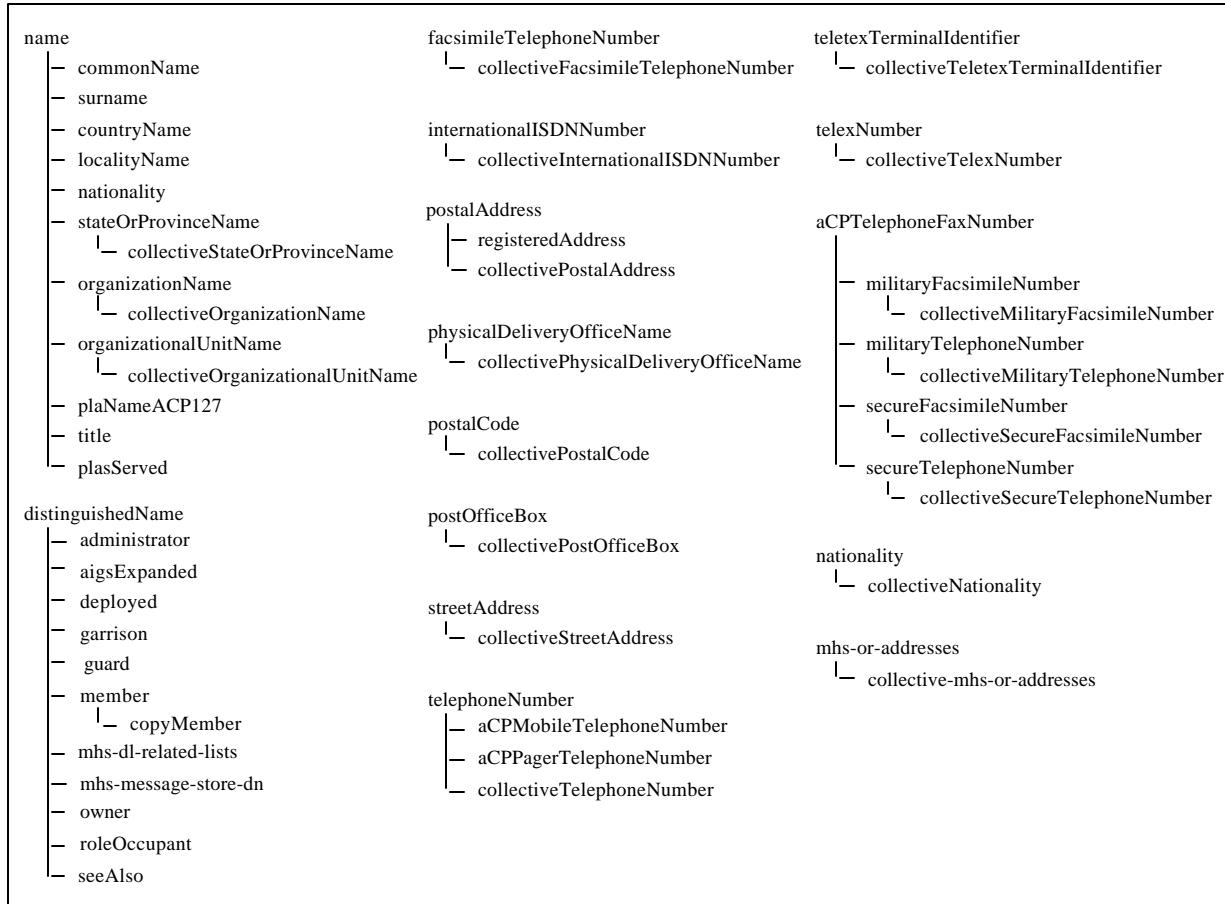


Figure B-2
Attribute Types Defined by Subtyping

SECTION VII

USEFUL OBJECT CLASSES AND NAME FORMS

15. General

There are no object classes defined in this ACP besides the ones included in the Common Content. There are no name forms defined in this ACP besides the ones that apply to the structural object classes included in the Common Content.

SECTION VIII

USEFUL ATTRIBUTES

16. General

a. Some useful attributes have been defined in RFC 1274. Useful attributes defined in paragraph 209 of this Annex are:

- collectiveMilitaryPostalAddress
- collectiveVisitorAddress
- hoursOfOperation
- jpegPhoto
- militaryPostalAddress
- visitorAddress

b. Useful attributes shall not be replicated unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

SECTION IX

ATTRIBUTE DEFINITIONS

17. Common Content

The following paragraphs define the attributes that are included in the Common Content. The definitions of attributes defined in the referenced standards are included for convenience only, and the definitions in those standards take precedence over those given here.

18. accessCodes

a. The accessCodes attribute value gives the coding of how to reach one network from another. Additional instructions for the use of this access code are contained in a description attribute in the same entry. For example, in a private telephone network, the user could be required to dial “8” to reach other users in a different city or to dial “9” to exit the private network.

b. This attribute is defined in this ACP.

19. accessSchema

a. The accessSchema attribute value is a schematic representation used to complete the access information from one network to another in the case of a complex connection. (Many connections are not complex enough to need such a description and in that case the attribute would not be populated.)

b. This attribute is defined in this ACP. Note that this attribute is replaced by the aCPNetwAccessSchemaEdB attribute.

20. accountingCode

a. The accountingCode attribute value is a character string used in logistics applications to identify an organization uniquely. One example is the U.S. Department of Defense Activity Accounting Code (DODAAC).

b. This attribute is defined in this ACP.

21. aCPLegacyFormat

a. The aCPLegacyFormat provides the specific message format type used when the value of the aCPPREFERREDDELIVERY attribute is ACP127(1). The values are:

- JANAP 128
- ACP 126
- DOI 103
- DOI 103 Special
- ACP 127
- ACP 127 Converted
- Reserved1 for ACP 127 Standard
- ACP 127 State
- ACP 127 Modified
- SOCOMM Special
- SOCOMM Narrative
- Reserved2 for SOCOMM Narrative TTY
- SOCOMM Narrative Special
- SOCOMM Data
- SOCOMM Internal
- SOCOMM External
- several values for national or bilateral use

b. This attribute is defined in this ACP.

22. aCPMobileTelephoneNumber

- a. The aCPMobileTelephoneNumber attribute value identifies a mobile telephone number for the object represented by the directory entry that contains this attribute.
- b. This attribute is a subtype of telephoneNumber and is defined in this ACP.

23. aCPNetwAccessSchemaEdB

- a. The aCPNetwAccessSchemaEdB attribute value is a schematic representation used to complete the access information from one network to another in the case of a complex connection. (Many connections are not complex enough to need such a description and in that case the attribute would not be populated.)
- b. This attribute is defined in this ACP. Note that this attribute replaces the accessSchema attribute.

24. aCPNetworkSchemaEdB

- a. The aCPNetworkSchemaEdB attribute value is a graphical representation of a network. It describes the structure of the network and details any rules associated with that network.
- b. This attribute is defined in this ACP. Note that this attribute replaces the networkSchema attribute.

25. aCPPagerTelephoneNumber

- a. The aCPPagerTelephoneNumber attribute identifies a telephone number for a pager associated with the object represented by the directory entry.
- b. This attribute is a subtype of telephoneNumber and is defined in this ACP.

26. aCPPREFERREDDELIVERY

- a. The aCPPREFERREDDELIVERY attribute value is used to determine the messaging system that a user, represented by the directory entry, prefers for message delivery. The possible values are: "ACP127", "SMTP" or "MHS". The "MHS" value signifies either standard X.400 (1984 or 1988) or ACP 123-compliant X.400. When the value is "ACP127" more information is given in the aCPLegacyFormat attribute (see paragraph 21 of this annex).
- b. This attribute is defined in this ACP.

27. aCPTelephoneFaxNumber

a. The aCPTelephoneFaxNumber attribute is defined for use as a supertype in defining the attributes:

- militaryFacsimileNumber
- militaryTelephoneNumber
- secureFacsimileNumber
- secureTelephoneNumber

b. A value of the aCPTelephoneFaxNumber attribute and the attributes defined as its subtypes is a telephone number that is used for military purposes and is associated with an object represented by the directory entry. For example, a person may have a telephone, equipped with a STU III device, on the Public Switched Telephone Network (PSTN).

c. The attribute value for an ACP telephone number contains the following substrings which are separated by commas (i.e., ","):

- network or site identifier
- telephone number
- security device identifier

(1) The maximum size of the network or site identifier substring is 6 characters. In the example, the string "PSTN" would be the value of this identifier.

(2) For the telephone number substring, if the network is the PSTN, then the format shall be as for a Telephone Number as defined in X.520 (i.e., CCITT E.123). Extension numbers shall be preceded by "ext." or other nationally defined equivalent. The maximum length of this substring is 32 characters. In the example, the string "+1 555 222 ext. 34" could be the value of the telephone number.

(3) The maximum size of the security device identifier substring is 8 characters. In the example, the string "STU III" would be the value of this identifier.

d. The complete example value would be "PSTN, +1 555 222 ext. 34, STU III".

e. The security device (and preceding substring separator ",") is present only if the military telephone number is secured (i.e., attribute subtypes secureTelephoneNumber or secureFacsimileNumber).

f. Note that the equality and substring matching rule for this attribute is not case sensitive and the substring matching rule is case sensitive. Thus, it is recommended that the network/site identifier and security device identifier are in upper case.

g. This attribute is defined in this ACP.

28. actionAddressees

a. An actionAddressees attribute value is the list of action addressees of an ACP 127/JANAP 128 collective, for example an Address Indicator Group. An action addressee is expected to take appropriate action on the message content, whereas an information addressee receives the message for informational purposes only.

b. This attribute is defined in this ACP.

29. additionalAddressees

a. The additionalAddressees attribute value is a list of addressees to be added to the actionAddressees list (value of the actionAddressees attribute) under circumstances identified in the remarks attribute in the same directory entry.

b. This attribute is defined in this ACP.

30. additionalSecondPartyAddressees

a. The additionalSecondPartyAddressees attribute value is a list of addressees to be added to the secondPartyAddressees list (value of the secondPartyAddressees attribute) under circumstances identified in the remarks attribute in the same directory entry.

b. This attribute is defined in this ACP.

31. adminConversion

a. The adminConversion attribute provides for using an abbreviation of the organization's administrative title as an administrative message address.

b. This attribute is defined in this ACP.

32. administrator

a. The administrator attribute value represents the entity responsible for the operation of a component when it is different from the owner of the component. For example, the owner may be a domain.

b. This attribute is defined in this ACP.

33. aigsExpanded

a. The aigsExpanded attribute values are the names of the AIGs expanded by a messaging gateway.

b. This attribute is defined in this ACP.

34. aLEXemptedAddressProcessor

a. The aLEXemptedAddressProcessor attribute value is the ORName of the address list's exempted address processor.

b. This attribute is defined in this ACP.

35. aliasedEntryName

a. The aliasedEntryName attribute value contains a name of the directory entry to which the object containing this attribute refers.

b. This attribute is defined in X.501.

36. aliasPointer

a. The aliasPointer attribute type value points to alias directory entries which might have to be modified if the directory entry containing this attribute is modified. It is intended to be used to maintain data consistency in the Directory Information Base (DIB).

b. This attribute is defined in this ACP.

37. alid

a. The alid attribute value is the AL key material identifier.

b. This attribute is defined in this ACP.

38. allowableOriginators

a. The allowableOriginators attribute value is the name of an ACP 127/JANAP 128 collective that contains the list of PLAs that are allowed to originate messages to this list.

b. This attribute is defined in this ACP.

39. aLReceiptPolicy

a. The aLReceiptPolicy attribute value indicates address list's signed receipt policy. This receipt policy supersedes the originator's request for signed receipts (see ACP 120).

b. This attribute is defined in this ACP.

40. alternateRecipient

a. The alternateRecipient attribute is used to designate an X.400 alternate recipient for a messaging user. It could be used by an X.400 message originator to create an originator-assigned alternate recipient address to be used by the message transfer system if delivery to the addressed recipient fails.

b. This attribute is defined in this ACP.

41. aLType

a. The aLType attribute value indicates the type of an address list from these possibilities: AIG (Address Indicator Group), Type Organization Collective, CAD (Collective Address Designator), Task Force, and DAG (DSSCS Address Group).

b. This attribute is defined in this ACP.

42. aprUKMs

a. The aprUKMs (User Key Materials) attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of April.

b. This attribute is defined in this ACP.

43. associatedAL

a. The associatedAL attribute value points to the address list object which replaces the ACP 127/JANAP 128 Task Force PLA. It assists in the transition from ACP 127/JANAP 128 to X.400 addressing and the associated transition from the use of ACP 127/JANAP 128 collectives to the use of address lists.

b. This attribute is defined in this ACP.

44. associatedOrganization

a. The associatedOrganization attribute value points to the Organizational Unit Ed. B directory entry which represents the same organizational messaging entity as the PLA directory entry containing this attribute.

b. This attribute is defined in this ACP.

45. associatedPLA

a. The associatedPLA attribute value points to the ACP 127/JANAP 128 directory entry for the same messaging entity as represented by the Organizational Unit Ed. B directory entry containing this attribute.

b. This attribute is defined in this ACP.

46. attributeCertificate

a. The attributeCertificate attribute is used to issue new authorizations from a Certification Authority (CA) other than the CA who originally issued the user certificate. The attribute certificate is bound to a user's X.509 certificate but is not part of the originally issued user certificate.

- b. This attribute is defined in ITU-T Rec. X.509 (1997).

47. augUKMs

- a. The augUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of August.

- b. This attribute is defined in this ACP.

48. authorityRevocationList

- a. The authorityRevocationList value is a time-stamped list of revoked certificates of all CAs known to the CA, certified by the CA.

- b. This attribute is defined in X.509.

49. buildingName

- a. The buildingName attribute value is the name of the building in which an organizational unit is based.

- b. This attribute is defined in RFC 1274.

50. businessCategory

- a. The businessCategory attribute value specifies information concerning the occupation of a person, providing the facility for interrogating the directory about people sharing the same occupation.

- b. This attribute is defined in X.520.

51. cACertificate

- a. The cACertificate attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

- b. The definition of realm is purely a matter of local policy.

- c. This attribute is defined in X.509.

52. certificateRevocationList

- a. The certificateRevocationList attribute value is a time-stamped list of the certificates the Certification Authority issued which have been revoked.

- b. This attribute is defined in X.509.

53. cognizantAuthority

a. The cognizantAuthority attribute value indicates the administrator for an ACP 127/JANAP 128 collective.

b. This attribute is defined in this ACP.

54. commonName

a. A commonName attribute value is an identifier of a person, role, or other object. A Common Name is not necessarily part of a directory name although this attribute is used in naming in the Allied Directory DIT. A Common Name is a (possibly ambiguous) name by which the object is commonly known in some limited scope (such as an organization) and conforms to the naming conventions of the country or culture with which it is associated. For example:

- commonName = “Eisenhower, Dwight”
- commonName = “Divisional Commander”
- commonName = “High Speed Modem”

b. Any variants associated with the named object are separate and alternative attribute values (i.e., the commonName attribute is multi-valued in the object’s entry).

c. This attribute is defined in X.520.

55. community

a. The community attribute value indicates whether an object belongs to the GENSER (R) or SI (Y) community or both (R/Y).

b. This attribute is defined in this ACP.

56. copyMember

a. The copyMember attribute value specifies a group of names associated with the object represented by the directory entry. In an Address List Ed. A directory entry, this attribute indicates the “copy” or “info” members of the list as opposed to “primary” or “action” members.

b. This attribute is defined in this ACP.

57. countryName

a. The countryName attribute value specifies a country. When used as a component of a directory name, it identifies the country in which the named object is physically located or with which it is associated in some other important way.

b. This attribute is defined in X.520.

58. crossCertificatePair

a. The forward elements of the crossCertificatePair attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the crossCertificatePair attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the forward and the reverse elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

b. When a reverse element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

c. In the case of V3 certificates, none of the above CA certificates shall include a basicConstraints extension with the cA value set to FALSE.

d. The definition of realm is purely a matter of local policy.

e. This attribute is defined in X.509 (1997).

59. decUKMs

a. The decUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of December.

b. This attribute is defined in this ACP.

60. deltaRevocationList

a. The deltaRevocationList attribute value is a partial certificateRevocationList (CRL) indicating only changes since the prior CRL issue.

b. This attribute is defined in X.509 (1997).

61. deployed

a. The deployed attribute value contains distinguished names of other directory entries that represent the same real world object in the field. See the garrison attribute.

b. This attribute is defined in this ACP.

62. description

a. The description attribute value specifies a text string which describes the associated object.

b. This attribute is defined in X.520.

63. destinationIndicator

a. The destinationIndicator attribute value specifies (in accordance with CCITT Recommendation F.1 and CCITT Recommendation F.31) the country and city associated with the object (the addressee) in order to provide the Public Telegram Service.

b. This attribute is defined in X.520.

64. distinguishedName

a. The distinguishedName attribute type is the attribute supertype from which attribute types, that specify the (directory) name of an object, are formed. The attributes in Common Content that are subtypes of distinguishedName are: administrator, aigsExpanded, deployed, garrison, guard, member, mhs-dl-related-lists, mhs-message-store-dn, owner, roleOccupant, and seeAlso.

b. This attribute is defined in X.520.

65. distributionCodeAction

a. The distributionCodeAction attribute values identify the distribution codes (including Subject Indicator Codes (SICs)) for which an organization, person, or role handles messages for action.

b. This attribute is defined in this ACP.

66. distributionCodeInfo

a. The distributionCodeInfo attribute values identify the distribution codes (including SICs) for which an organization, person, or role handles messages for information.

b. This attribute is defined in this ACP.

67. dnQualifier

a. The dnQualifier attribute value is used as part of a RDN to distinguish between directory entries for different objects..

b. This attribute is defined in X.520.

68. dualRoute

a. The dualRoute attribute value indicates whether delivery of messages for an organization to both the home and deployed sites is required. If set to TRUE, dual delivery is required.

b. This attribute is defined in this ACP.

69. effectiveDate

a. The effectiveDate attribute value indicates when the directory entry is to become valid.

b. This attribute is defined in this ACP.

70. enhancedSearchGuide

The enhancedSearchGuide attribute is defined in X.520, but is not used to meet Allied Directory requirements.

71. entryClassification

a. The entryClassification attribute value indicates the classification of the directory entry that contains this attribute. The possible values are: unmarked, unclassified, restricted, confidential, secret, and top secret.

b. This attribute is defined in this ACP.

72. expirationDate

a. The expirationDate attribute value indicates the time at which the directory entry becomes invalid.

b. This attribute is defined in this ACP.

73. facsimileTelephoneNumber

a. The facsimileTelephoneNumber attribute value specifies a telephone number for a facsimile terminal (and optionally its parameters) associated with the object represented by the directory entry.

b. An attribute value for the facsimileTelephoneNumber is a string that complies with the internationally agreed format for showing international telephone numbers, CCITT Recommendation E.123 (e.g., "+81 3 347 7418") and an optional bit string (formatted according to CCITT Recommendation T.30).

c. This attribute is defined in X.520.

74. febUKMs

a. The febUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of February.

b. This attribute is defined in this ACP.

75. garrison

a. The garrison attribute value contains distinguished names of other directory entries that represent the same real world object in garrison. See the deployed attribute.

b. This attribute is defined in this ACP.

76. gatewayType

a. The gatewayType attribute value is used to indicate the translations a messaging gateway is capable of performing. The translations that can be indicated are:

- acp120-acp127-gateway
- acp120-janap128-gateway
- acp120-mhs-gateway
- acp120-mmhs-gateway
- acp120-rfc822-gateway
- boundary MTA
- mmhs-mhs-gateway
- mmhs-rfc822-gateway
- mta-acp127-gateway

b. This attribute is defined in this ACP.

c. For the ACP120-acp127 translation, the messaging gateway performs the changes that are necessary to exchange messages between an acp120 organization and an acp127 organization.

77. generationQualifier

The generationQualifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

78. ghpType

a. The ghpType attribute value is used to indicate the gateway handling policy of an mta-acp127-gateway defined in STANAG 4406.

b. This attribute is defined in this ACP.

79. givenName

The givenName attribute is defined in X.520, but is not used to meet Allied Directory requirements.

80. guard

- a. The guard attribute value indicates the Name(s) of the Guard Gateway.
- b. This attribute is defined in this ACP.

81. host

- a. The host attribute value gives an identifier for a host computer.
- b. This attribute is defined in the COSINE and Internet X.500 Schema, RFC 1274.

82. hostOrgACP127

a. The hostOrgACP127 attribute value of a tenant PLA identifies the PLA for the organization which accepts traffic for a tenant.

- b. This attribute is defined in this ACP.

83. houseIdentifier

The houseIdentifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

84. infoAddressees

a. The infoAddressees attribute value of an ACP 127/JANAP 128 collective contains the list of information addressees of the collective.

- b. This attribute is defined in this ACP.

85. initials

The initials attribute is defined in X.520, but is not used to meet Allied Directory requirements.

86. internationalISDNNumber

a. The internationalISDNNumber attribute value specifies an International Integrated Services Digital Network (ISDN) Number associated with (the object represented by) the directory entry.

- b. An attribute value for internationalISDNNumber is a string which complies with the internationally agreed format for ISDN addresses given in CCITT Recommendation E.164.

c. This attribute is defined in X.520.

87. janUKMs

a. The janUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of January.

b. This attribute is defined in this ACP.

88. julUKMs

a. The julUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of July.

b. This attribute is defined in this ACP.

89. junUKMs

a. The junUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of June.

b. This attribute is defined in this ACP.

90. knowledgeInformation

a. The knowledgeInformation attribute value specifies a human readable description of knowledge mastered by a specific DSA.

b. This attribute is defined in X.520 but has been superseded by operational knowledge attributes defined in the 1993 edition of the standard. (See 196 b and 198 b in this annex.)

91. lastRecapDate

a. The lastRecapDate attribute value indicates when a list was last recapped or validated.

b. This attribute is defined in this ACP.

92. listPointer

a. The listPointer attribute value is used to point to Address List Ed. A directory entries which might have to be modified if the entry containing this attribute is modified. It is intended to be used to maintain data consistency in the DIB.

b. This attribute is defined in this ACP.

93. lmf

a. The lmf (Language and Media Format) attribute value indicates the language and media format that can be accepted between the two communicating end-systems. Possible values include:

- T tape
- A ASCII (American Standard Code for Information Interchange)
- C card, etc.

b. This attribute is defined in this ACP.

94. localityName

a. The localityName attribute value identifies a geographical area or locality in which the object represented by the directory entry is physically located or with which the object is associated in some other important way.

b. This attribute is defined in X.520.

95. longTitle

a. The longTitle attribute value is the expanded form of an organization's PLA.

b. This attribute is defined in this ACP.

96. mailDomains

a. The mailDomains attribute value is a string, which provides information on the domains that the messaging gateway will bridge.

b. This attribute is defined in this ACP.

97. marUKMs

a. The marUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of March.

b. This attribute is defined in this ACP.

98. mayUKMs

a. The mayUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of May.

b. This attribute is defined in this ACP.

99. member

a. The member attribute value specifies a group of names associated with the object represented by the directory entry. In an Address List Ed. A directory entry, this attribute indicates the “primary” or “action” members of the list as opposed to “copy” or “info” members.

b. This attribute is defined in X.520.

100. mhs-acceptable-eits

a. The mhs-acceptable-eits attribute value identifies a set of encoded information types (EITs) for messages. The user or distribution list, represented by the directory entry, will accept delivery of or expand a message in which any one of these EITs is present.

b. This attribute is defined in X.402.

101. mhs-deliverable-classes

a. The mhs-deliverable-classes attribute value identifies the classes of messages whose delivery a UA, represented by the directory entry, will accept.

b. This attribute is defined in X.402.

102. mhs-deliverable-content-types

a. The mhs-deliverable-content-types attribute values identify the content types of the messages whose delivery the user, represented by the directory entry, will accept.

b. This attribute is defined in X.402.

103. mhs-dl-archive-service

a. The mhs-dl-archive-service attribute value identifies a service from which a user may request copies of messages previously distributed by the address list represented by the directory entry.

b. This attribute is defined in X.402.

104. mhs-dl-members

a. The mhs-dl-members attribute value is an OR-name which identifies a member of the DL. This attribute may have multiple values each of which identifies one member of the DL. When a DL is expanded, each of the values of this attribute becomes a recipient of the message.

b. This attribute is defined in X.402.

105. mhs-dl-policy

- a. The mhs-dl-policy attribute value identifies the choice of policy options to be applied when expanding the address list represented by the directory entry.
- b. This attribute is defined in X.402.

106. mhs-dl-related-lists

- a. The mhs-dl-related-lists attribute value identifies other address lists which are, in some unspecified way, related to the address list represented by the directory entry.
- b. This attribute is defined in X.402.

107. mhs-dl-submit-permissions

- a. The mhs-dl-submit-permissions attribute values identify the users and address lists that may submit messages to the address list represented by the directory entry.
- b. This attribute is defined in X.402.

108. mhs-dl-subscription-service

- a. The mhs-dl-subscription-service attribute value identifies a service of which a user may request changes to the membership of the address list represented by the directory entry, (e.g., for a user to request to be added to the address list).
- b. This attribute is defined in X.402.

109. mhs-exclusively-acceptable-eits

- a. The mhs-exclusively-acceptable-eits attribute value identifies a set of EITs for messages. The user or distribution list, represented by the directory entry, will accept delivery of or expand a message in which all of these EITs is present.
- b. This attribute is defined in X.402.

110. mhs-maximum-content-length

- a. The mhs-maximum-content-length attribute value identifies the maximum content length of the messages that can be handled by the object represented by the directory entry. The object is a user to whom the message would be delivered, an address list for which expansion would be performed on the message, or an MTA to which the message would be acceptable.
- b. This attribute is defined in X.402.

111. mhs-message-store-dn

a. The mhs-message-store-dn attribute value identifies by directory name the message store of the user represented by the directory entry.

b. This attribute is defined in X.402.

112. mhs-or-addresses

a. The mhs-or-addresses attribute values specify the O/R addresses of the user or address list represented by the directory entry.

b. This attribute is defined in X.402.

113. mhs-or-addresses-with-capabilities

a. The mhs-or-addresses-with-capabilities attribute values specify the O/R addresses and the messaging capabilities associated with each address of the user or address list represented by the directory entry.

b. Recognized security labels are identified in ACP 123.

c. Information about availability and nationality will be included in the description.

If the address is served by a foreign nation, the International Organization for Standardization 3166 code of the country shall be entered first.

d. If an OR-address is not operational on a 24 by 7 basis, the normal daily schedule shall be given in start and stop times for each day of operation. Planned down time also shall be given in start and stop time.

e. This attribute is defined in X.402.

114. mhs-supported-attributes

a. The mhs-supported-attributes attribute values identify the attributes the message store, represented by the directory entry, fully supports.

b. This attribute is defined in X.402.

115. mhs-supported-automatic-actions

a. The mhs-supported-automatic-actions attribute values identify the automatic actions that the message store, represented by the directory entry, supports.

b. This attribute is defined in X.402.

116. mhs-supported-content-types

a. The mhs-supported-content-types attribute values identify the content types of the messages whose syntax and semantics the message store, represented by the directory entry, supports.

b. This attribute is defined in X.402.

117. mhs-supported-matching-rules

a. The mhs-supported-matching-rules attribute values identify the matching rules the message store, represented by the directory entry, fully supports.

b. This attribute is defined in X.402.

118. mhs-unacceptable-eits

a. The mhs-undeliverable-eits attribute value identifies the encoded information types of a message which would make a user not accept delivery, or which would prevent an address list from doing expansion on the message. The absence of this attribute indicates that there are no EITs which are unacceptable. The presence of the special value “id-eit-all” indicates that all EITs are unacceptable except for those EITs identified by the mhs-acceptable-eits or mhs-exclusively-acceptable-eits attribute.

b. This attribute is defined in X.402.

119. militaryFacsimileNumber

a. The militaryFacsimileNumber attribute value identifies a military facsimile number, such as a Defense Switched Network (DSN) number or Defence Fixed Telecommunications Service (DFTS) number, which is associated with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a militaryFacsimileNumber value is “DFTS, 555 1111 ext 25”.

c. This attribute is defined in this ACP.

120. militaryTelephoneNumber

a. The militaryTelephoneNumber attribute value identifies a military telephone number, such as a DSN number, which is associated with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a militaryTelephoneNumber value is “DSN, 555-333”.

c. This attribute is defined in this ACP.

121. minimize

- a. The minimize attribute value indicates whether an organization, person, or role, represented by the directory entry, is under the MINIMIZE condition. If so, the message originators are responsible for not sending unnecessary messages to the recipient.
- b. This attribute is defined in this ACP.
- c. Currently, the minimize attribute is not employed.

122. minimizeOverride

- a. The minimizeOverride attribute value is used by the Message Conversion System (MCS) to determine whether the MINIMIZE condition will be enforced when a message is originated by this PLA. If the value is FALSE, override does not occur and MINIMIZE is enforced. If the value is TRUE, MINIMIZE is not enforced.
- b. This attribute is defined in this ACP.
- c. Currently, the minimizeOverride attribute is not employed.

123. name

- a. The name attribute type is the attribute supertype from which string attribute types used for naming are formed. The attributes in Common Content that are subtypes of name are: commonName, surname, countryName, localityName, nationality, stateOrProvinceName, organizationName, organizationalUnitName, plaNameACP127, plasServed, and title.
- b. This attribute is defined in X.520.

124. nameClassification

- a. The nameClassification attribute value indicates the security classification of the name of the directory entry itself.
- b. This attribute is defined in this ACP.

125. nationality

- a. The nationality attribute value names the country which "owns" an entity. For an individual, it would be the nationality of the person. The standard Country Name attribute is used to denote the location of the entity.
- b. This attribute is defined in this ACP.

126. networkDN

a. The networkDN attribute value contains the full DN of a network and may be used to reference the entry for the network from another entry (e.g., used in the Network Instructions Ed. B entry to reference the entry for the accessed network).

b. This attribute is defined in this ACP.

127. networkSchema

a. The networkSchema attribute value is a graphical representation of a network. It describes the structure of the network and details any rules associated with that network.

b. This attribute is defined in this ACP. Note that this attribute is replaced by the aCPNetworkSchemaEdB attribute.

128. novUKMs

a. The novUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of November.

b. This attribute is defined in this ACP.

129. octUKMs

a. The octUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of October.

b. This attribute is defined in this ACP.

130. onSupported

a. The onSupported attribute value indicates the types of notifications, besides MHS notifications, generated by an mta-acp127-gateway type of gateway. The gateway may generate all or none of the notifications. If the attribute is absent, the gateway does none of the notifications.

b. This attribute is defined in this ACP.

131. operationName

a. The operationName attribute value is the name of an official military operation. For example, when used in the definition of a network (i.e., in a Network directory entry), it could be the TURQUOISE operation which develops a RITA network.

b. This attribute is defined in this ACP.

132. organizationalUnitName

a. The organizationalUnitName attribute value specifies an organizational unit. When used as a component of a directory name, it identifies an organizational unit with which the named directory entry is affiliated. The designated organizational unit is understood to be part of an organization designated by an organizationName attribute value. It follows that, if an organizationalUnitName attribute value is used in a directory name, it must be associated with an organizationName attribute value.

b. An attribute value for organizationalUnitName is a string chosen by the organization of which it is part (e.g., OU = "Technology Division"). Note that the commonly used abbreviation "TD" would be a separate and alternative attribute value. Example: O = "Scottel", OU = "TD".

c. This attribute is defined in X.520.

133. organizationName

a. The organizationName attribute type value identifies an organization. When used as a component of a directory name, it identifies an organization with which the named directory entry is affiliated.

b. An attribute value for organizationName is a string chosen by the organization (e.g. O = "Scottish Telecommunications plc"). Any variants should be associated with the named organization as separate and additional attribute values.

c. This attribute is defined in X.520.

134. owner

a. The owner attribute value specifies the name of some object which has some responsibility for the directory entry that contains this attribute. An attribute value for owner is a distinguished name (which could represent a group of names) and can have several values.

b. This attribute is defined in X.520.

135. physicalDeliveryOfficeName

a. The physicalDeliveryOfficeName attribute value specifies the name of the city, village, etc. where the physical delivery office, that serves the object represented by the directory entry, is situated. An attribute value for physicalDeliveryOfficeName is a string.

b. This attribute is defined in X.520.

136. plaAddressees

a. The plaAddressees attribute value of an ACP 127/JANAP 128 collective contains the list of action and information addressees of the collective. It is used for some types of collectives instead of separating action and information addressees.

b. This attribute is defined in this ACP.

137. plaNameACP127

a. The plaNameACP127 attribute value is the object's (represented by the directory entry) ACP 127/JANAP 128 plain language address. A PLA is sometimes called the Signal Message Address or registered PLA. The long form of the PLA name is represented in the ACP 133 by the longTitle attribute.

b. This attribute is defined in this ACP.

138. plaReplace

a. The plaReplace attribute value is used by ACP 127/JANAP 128. When an "alternate spelling" PLA is addressed on a message, the MCS will look at the value of this attribute in the PLA's directory entry. If set, the alternate spelling on the message will be replaced with the "primary" or correct spelling. (Each alternate spelling has a pointer to the primary PLA.)

b. This attribute is defined in this ACP.

139. plasServed

a. The plasServed attribute value is a list of the PLAs accessible through a gateway.

b. This attribute is defined in this ACP.

140. positionNumber

a. The position number attribute value is used by government and Defense agencies to identify uniquely each individual's position, and possibly role and duties, within the organization.

b. This attribute is defined in this ACP.

141. postalAddress

a. The postalAddress attribute value is the address information required for the physical delivery of postal messages by the postal authority to the object represented by the directory entry. An attribute value for Postal Address will typically be composed of selected attributes from the MHS Unformatted Postal O/R Address version 1 according to CCITT Recommendation F.401 and limited to 6 lines of 30 characters each, including a Postal Country Name. Normally, the information contained in such an address could include an addressee's name, street address,

city, state or province, postal code and possibly a Post Office Box number depending on the specific requirements of the object.

- b. This attribute is defined in X.520.

142. postalCode

a. The postalCode attribute value specifies the postal code of the object represented by the directory entry. If this attribute value is present it will be part of the object's postal address.

- b. This attribute is defined in X.520.

143. postOfficeBox

a. The postOfficeBox attribute value is the identifier of the Post Office Box at which the object, represented by the directory entry, receives physical postal delivery. If present, the attribute value is part of the object's postal address.

- b. This attribute is defined in X.520.

144. preferredDeliveryMethod

a. The preferredDeliveryMethod attribute value indicates the priority order regarding the method to be used for communicating with the object represented by the directory entry. The possible methods that may be indicated in a value of this attribute are:

- any-delivery-method,
- mhs-delivery,
- physical-delivery,
- telex-delivery,
- teletex-delivery,
- g3-facsimile-delivery,
- g4-facsimile-delivery,
- ia5-terminal-delivery,
- videotex-delivery,
- telephone-delivery

- b. This attribute is defined in X.520.

145. presentationAddress

- a. The presentationAddress attribute value specifies a presentation address associated with an application entity object, represented by the directory entry.
- b. This attribute is defined in X.520.

146. primarySpellingACP127

- a. The primarySpellingACP127 attribute value of an Alternate Spelling PLA directory entry is the object's correct PLA spelling.
- b. This attribute is defined in this ACP.

147. proprietaryMailboxes

- a. The proprietaryMailboxes attribute value identifies a mail box identifier that can be used to address mail within the local proprietary domain, such as cc:mail.
- b. This attribute is defined in this ACP.

148. protocolInformation

- a. The protocolInformation attribute value indicates the associated protocol information for each network address in the presentationAddress attribute.
- b. This attribute is defined in X.520.

149. publish

- a. The publish attribute value indicates whether this PLA should be published in the Message Address Directory or the ACP 117. Access controls may be set based on this attribute.
- b. This attribute is defined in this ACP.

150. rank

- a. The value of the rank attribute type contains the military or civilian rank of an individual such as Major or civilian grade.
- b. This attribute is defined in this ACP.

151. recapDueDate

- a. The recapDueDate attribute value indicates when a list is expected to be recapped or validated.
- b. This attribute is defined in this ACP.

152. registeredAddress

a. The registeredAddress attribute value is a mnemonic for an address associated with an object at a particular city location. The mnemonic is registered in the country in which the city is located and is used in the provision of the Public Telegram Service (according to CCITT Recommendation F.1).

b. This attribute is defined in X.520.

153. releaseAuthorityName

a. The releaseAuthorityName attribute value is a relative distinguished name of a release authority for an organization.

b. This attribute is defined in this ACP.

154. remarks

a. The remarks attribute value is textual information associated with a PLA's directory entry. These remarks may be instructions rather than a description of the entity.

b. This attribute is defined in this ACP.

155. rfc822Mailbox

a. The rfc822Mailbox attribute value is an electronic mailbox identifier following the syntax in RFC 822. An example for a user on a military network is "user@host.Service.mil".

b. This attribute is defined in the COSINE/Internet schema, RFC 1274.

156. rI

a. The rI (Routing Indicator) attribute value is the information mapped to in ACP 127/JANAP 128 from a user's PLA name. Users are named by their PLA names and delivered to by their routing indicator values, analogous to Directory Names and O/R Addresses for X.400 users.

b. This attribute is defined in this ACP.

157. rIClassification

a. The rIClassification attribute value indicates the highest classification of data allowed to be processed by a specified device.

b. This attribute is defined in this ACP.

158. rIInfo

a. The rIInfo attribute value is RI values with the associated properties of each RI.

- b. This attribute is defined in this ACP.

159. roleOccupant

- a. The roleOccupant attribute value is the distinguished name of a directory entry that represents the person or organizational unit who fulfills an organizational role.

- b. This attribute is defined in X.520.

160. roomNumber

- a. The roomNumber attribute value identifies a room number.

- b. This attribute is defined in the COSINE/Internet schema, RFC 1274.

161. searchGuide

- a. The searchGuide attribute value specifies suggested search criteria which may be included in some entries expected to be convenient base-objects for search operations, e.g., Country or Organization.

- b. Search criteria consist of an optional identifier for the type of object sought and combinations of attribute types and logical operators to be used in the construction of a filter. It is possible to specify for each search criteria item the matching level, e.g., approximate match.

- c. The searchGuide attribute value may have multiple values to reflect the various types of requests, e.g., search for a Residential Person or an Organizational Person, which may be fulfilled from the directory entry where the Search Guide is read.

- d. This attribute is defined in X.520.

162. secondPartyAddressees

- a. The secondPartyAddressees attribute value is a list of second party action PLAs.

- b. This attribute is defined in this ACP.

163. section

- a. The section attribute value is set to TRUE if the receiving PLA requires message sectioning to be performed. This is required to transition users with slow-speed terminals.

- b. This attribute is defined in this ACP.

164. secureFacsimileNumber

- a. The secureFacsimileNumber attribute value is a facsimile number that is used for secure communication with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a secureFacsimileNumber value is “DSN, 555-333”.

c. This attribute is defined in this ACP.

165. secureTelephoneNumber

a. The secureTelephoneNumber attribute value is a telephone number of a secure device, such as STU II or STU III, that is used for secure communication with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a secureTelephoneNumber value is “PSTN, +1 555 222, STU III”.

c. This attribute is defined in this ACP.

166. seeAlso

a. The seeAlso attribute value contains distinguished names of other directory entries which may be other aspects (in some sense) of the same real world object. For example, an Organizational Person Ed. B directory entry may include the distinguished names of the Organizational Role Ed. B directory entries which designate the organizational person as a role occupant. See paragraph 310 in Chapter 3 of this ACP.

b. This attribute is defined in X.520.

167. sepUKMs

a. The sepUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of September.

b. This attribute is defined in this ACP.

168. serialNumber

a. The serialNumber attribute value specifies an identifier, the serial number, of a device.

b. This attribute is defined in X.520.

169. serviceNumber

a. The serviceNumber attribute value is the staff identifier number used by government and defense agencies for purposes such as payroll references, medical records, human resources, and duty rosters.

b. This attribute is defined in this ACP.

170. serviceOrAgency

- a. The serviceOrAgency attribute value is an identifier of the Service or agency to which the PLA belongs.
- b. This attribute is defined in this ACP.

171. sHD

- a. The sHD (specialHandlingDesignator) attribute value is a string containing the special handling designator which an entity, address, or routing indicator can support.
- b. This attribute is defined in this ACP.

172. shortTitle

- a. The shortTitle attribute value is a PLA name used for Signal Intelligence (SIGINT) related communications.
- b. This attribute is defined in this ACP.

173. sigad

- a. The sigad (SIGINT Address) attribute value is a PLA name used for sensitive SIGINT related communications.
- b. This attribute is defined in this ACP.

174. spot

- a. The spot attribute value identifies a special project address list or collective.
- b. This attribute is defined in this ACP.

175. stateOrProvinceName

- a. The stateOrProvinceName attribute value indicates a state or province. When used as a component of a directory name, it identifies a geographical subdivision in which the object, represented by the directory entry, is physically located or with which the object is associated in some other important way.
- b. This attribute is defined in X.520.

176. streetAddress

- a. The streetAddress attribute value specifies a site for the local distribution and physical delivery in a postal address, i.e., the street name, place, avenue, and house number. When used as a component of a directory name, it identifies the street address at which the

object, represented by the directory entry, is located or with which the object is associated in some other important way.

- b. This attribute is defined in X.520.

177. supportedAlgorithms

- a. The supportedAlgorithms attribute value is used to list the algorithms supported by the user.

- b. This attribute is defined in X.509.

178. supportedApplicationContext

- a. The supportedApplicationContext attribute value is the object identifier(s) of an application context(s) that the object (an OSI application entity) supports.

- b. This attribute is defined in X.520.

179. surname

- a. The surname attribute value is the linguistic construct which normally is inherited by an individual from the individual's parent or assumed by marriage, and by which the individual is commonly known.

- b. This attribute is defined in X.520.

180. tARE

- a. The tARE (Telegraph Automatic Relay Equipment) attribute value is a flag that specifies delivery responsibility for a message that is received by an intermediary. The flag is set in the directory entry for the intended recipient.

- b. This attribute is defined in this ACP.

181. tCC

- a. The tCC (Transmission Control Code) attribute value specifies a message handling instruction used in the routing indicator.

- b. This attribute is defined in this ACP.

182. tCCG

- a. The tCCG (Transmission Control Code Group) attribute value specifies a group of message handling instructions used in the routing indicator.

- b. This attribute is defined in this ACP.

183. telephoneNumber

- a. The telephoneNumber attribute value specifies a number for a telephone (and optionally its parameters) associated with the object represented by the directory entry.
- b. An attribute value for telephoneNumber is a string that complies with the internationally agreed format for showing international telephone numbers, CCITT Recommendations E.123 (e.g., "+44 582 10101").
- c. An extension should be indicated by writing the nationally used word or abbreviation for "extension" immediately after the telephone number, followed by the extension number itself. For example: "+22 607 123 4567 ext. 876."
- d. This attribute is defined in X.520.

184. teletexTerminalIdentifier

- a. The teletexTerminalIdentifier attribute value is the Teletex terminal identifier (and, optionally, parameters) for a teletex terminal associated with the object represented by the directory entry.
- b. An attribute value for teletexTerminalIdentifier is a string which complies with CCITT recommendation F.200 and an optional set whose components are determined according to CCITT recommendation T.62.
- c. This attribute is defined in X.520.

185. telexNumber

- a. The telexNumber attribute value is the telex number, country code, and answerback code of a telex terminal associated with the object represented by the directory entry.
- b. This attribute is defined in X.520.

186. title

- a. The title attribute value is the designated position or function of the object, represented by the directory entry, within an organization, e.g., Company Clerk.
- b. This attribute is defined in X.520.

187. transferStation

- a. The transferStation attribute value indicates whether a message for the entity should be sent to a communications processing and routing system, called a transfer station. For example, a Naval Communications Processing and Routing System (NAVCOMPARS) is a transfer station. If this attribute is TRUE, traffic should be routed to a transfer station.
- b. This attribute is defined in this ACP.

188. tRC

a. The tRC (Transmission Release Code) attribute value is the classification of data used in the routing indicator. Possible values include:

- A Australia
- B British Commonwealth less Canada, Australia, and New Zealand
- C Canada
- U US
- X Belgium, Denmark, France, Germany, Greece, Italy, Netherlands, Norway, Portugal, Turkey, NATO
- Z New Zealand

b. This attribute is defined in this ACP.

189. uniqueIdentifier

The uniqueIdentifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

190. uniqueMember

The uniqueMember attribute is defined in X.520, but is not used to meet Allied Directory requirements.

191. usdConversion

a. The usdConversion attribute value is an organizational address that is used when other types of address are not appropriate.

b. This attribute is defined in this ACP.

192. userCertificate

a. The userCertificate attribute contains the public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification of the certification authority that issued it.

b. This attribute is defined in X.509.

193. userPassword

a. A userPassword attribute value is the password used for simple authentication of the object represented by the directory entry.

- b. This attribute is defined in X.509.

194. x121Address

- a. The X.121 Address attribute value is an address, as defined by ITU-T Recommendation X.121, that is associated with the object represented by the directory entry.

- b. This attribute is defined in X.520.

195. Useful

The following paragraphs define attributes that may be useful, but are not part of the Common Content.

a. hoursOfOperation

- (1) A value of the hoursOfOperation attribute contains the scheduled hours of operation of an organizational unit.

- (2) This attribute is defined in this ACP.

b. jpegPhoto

- (1) A value of the jpegPhoto attribute is a JPEG image in the JPEG File Interchange Format (JFIF).

- (2) This attribute is defined in the inetOrgPerson Internet-Draft..

c. militaryPostalAddress

- (1) A value of the militaryPostalAddress attribute is an address assigned by a military authority and used by military postal services.

- (2) This attribute is defined in this ACP.

d. visitorAddress

- (1) A value of the visitorAddress attribute describes an address for visitors who want to access a site. It may also be used if the postal address is different from the physical address.

- (2) This attribute is defined in this ACP.

SECTION X

DIRECTORY SYSTEM SCHEMA

196. General

a. This subsection lists the information required for the Directory to know how to operate correctly. It specifies the type of information that is required in the Directory System Schema. The Directory System Schema consists of:

- definition of subentry object classes
- definition of Directory operational attributes

b. The Directory System Schema is distributed. Each administrative authority establishes the part of the system schema that will apply for those portions of the DIB administered by the authority. Each DSA participating in a directory system requires a full knowledge of the system schema established by its administrative authority. The Directory System Schema is not regulated by DIT structure or content rules and is normally viewed and controlled by the Directory Administrator or the DSA itself.

197. Standard Subentry Object Classes

The following subentry object classes are defined by X.501 and shall be supported by the ACP 133 Directory.

a. The subentry object class supports the Administrative and Operational Information Model of the Directory. The subentry object class is used to define the name and subtree for an access control, collective attribute, or subschema subentry of an administrative point.

b. The accessControlSubentry object class contains precisely one prescriptive Access Control Information attribute which contains access control information applicable to directory entries within that subentry's scope.

c. The collectiveAttributeSubentry shall contain at least one collective attribute which is available for interrogation and filtering at every entry within the scope of the subentry's Subtree Specification attribute.

d. The subschema object class is used to contain the operational attributes that represent the policy parameters used to express subschema policies (schema publication). The attributes include the rules and constraints concerning DIT structure, DIT content, object classes and attribute types, syntaxes, and matching rules which characterize the DIB.

198. Standard Operational Attributes

Operational attributes defined by X.500 and cited in this paragraph shall be supported by the ACP 133 Directory. The definition of an operational attribute includes a specification of the way in which the Directory uses and manages the attribute in the course of its operation. There

are two varieties of operational attribute: Directory operational attributes and DSA Specific Entry (DSE) operational attributes. Directory operational attributes occur in the Directory information model and are used to represent control information or other information provided by the Directory. DSE operational attributes are further categorized into two: DSA-shared operational attribute and DSA-specific operational attribute. They occur only in the DSA information model and are not visible at all in the Directory Information model.

a. Directory Operational Attributes

(1) The subtreeSpecification attribute shall be supported by the ACP 133 Directory. It supports the administrative and operational information model and is used to specify the scope of a subentry or area of replication. It is also used to regulate the subentries permitted to be subordinate to an administrative entry such as access control or collective attribute subentries.

(2) The administrativeRole attribute shall be supported by the ACP 133 Directory. It supports the administrative model and is used to indicate the role or roles of an administrative entry. The attribute may be stored in one or more of the following administrative points:

- Autonomous Administrative Point
- Access Control Administrative Point
- Access Control Inner Administrative Point
- Subschema Administrative Point
- Collective Attribute Administrative Point
- Collective Attribute Inner Administrative Point

(3) The attributes below, which may be contained in an entry or subentry, support general administrative and operational requirements. These attributes shall be supported by the ACP 133 Directory. All DSAs which conform to this ACP shall automatically provide date/time of creation/modification and creators/modifiers name on directory add and modify operations. Replication requires the use of createTimeStamp and modifyTimeStamp. The creatorsName and modifiersName are desirable for audit purposes.

- createTimeStamp
- modifyTimeStamp
- creatorsName
- modifiersName

(4) The collectiveExclusions attribute allows particular collective attributes to be excluded from an entry and shall be supported.

(5) The following attributes are used by the Security Model of the Directory and shall be supported:

- accessControlScheme,
- prescriptiveACI (Basic or Simplified Access Control),
- entryACI (Basic Access Control),
- subentryACI (Basic or Simplified Access Control)

(6) The accessControlScheme indicates which access control model, such as, Basic Access Control or Simplified Access Control, is in effect for an administrative area. It is placed in the Administrative Entry for the corresponding Administrative Point. The prescriptiveACI attribute is contained in an access control subentry. The entryACI, which may be used in Basic Access Control, is an operational attribute of an entry or subentry and contains access control information applicable to that entry. The subentryACI attribute is used in an administrative entry to provide access control information for subentries of the administrative point.

b. DSA Specific Entry (DSE) Operational Attributes

(1) Each directory entry in the DSA also contains additional attributes beyond what are visible to Directory administrator. The following attributes are operational attributes contained in DSEs. These attributes are used by the DSA Information Model and shall be supported by the ACP 133 Directory:

- dseType
- myAccessPoint
- superiorKnowledge
- specificKnowledge
- nonSpecificKnowledge
- supplierKnowledge
- consumerKnowledge
- secondaryShadows

(2) The dseType indicates the role or roles of a DSE, such as entry, subentry, or administrative point. The myAccessPoint attribute is an operational attribute used to represent its own access point and is contained in the root DSE. The information may be used by the DOP when establishing or modifying an operational binding. The superior, specific, and non-specific knowledge attributes are used by the DSA to find access points of DSAs for a naming context. The supplierKnowledge and consumerKnowledge attributes are used by the DSA to know the

access points and shadowing agreement identifiers of a replicated area. They are managed by the DSA itself. The secondaryShadows attribute is managed by the DSA itself and contains access points of consumer DSAs which are engaged in secondary shadowing.

(3) A DSE may have only the user attributes, the operational attributes or both depending on its role within the total DIB. Therefore, to identify an entry with its role and DIB location and its effect in the scheme of the total (and possibly distributed and replicated) DIB, a number of DSE entry types have been defined. Table B-50 defines the standard DSE types and their purpose. The DSE types shall be supported by this ACP for all DSAs in accordance with their definition.

Table B-55
DSE Types and Their Purpose

DSE Type	Purpose
root	Is the root of the DSA Information Tree.
glue	Represents knowledge of a name only. Used to connect the fragments of a DIT in shadowed copies, for example.
cp	Is the context prefix of a naming context, the root of a subtree.
entry	Holds an object entry, user information.
alias	Holds an alias entry.
subr	Holds a reference to a DSA holding a portion of the DIT subordinate to that in this DSA. Contains the context prefix of the subordinate.
nssr	Holds a non-specific subordinate reference to a DSA that holds some subordinate that is not named.
supr	Holds a superior reference, a DSA which holds a naming context superior in the DIT to all the naming contexts held by this DSA.
xr	Holds a cross reference to another DSA, used for optimization. Points directly to a remote naming context.
admpoint	Is an administrative point, the root vertex of an administrative area, a subtree of the DIT whose entries are all administered by the same Administrative Authority.
subentry	A subentry that is located under an administrative point and contains policy for access control, schema, and collective attributes.
shadow	Holds a shadow copy of an entry or part of an entry. Set by the shadow consumer.
immSupr	Holds a reference to a naming context immediately superior to the referencing one.
rhob	Holds information about a superior administrative point or subentry passed by a Relevant Hierarchical Operational Binding between DSAs.
sa	Subordinate reference DSE points to an alias entry.

199. Rules for DIT Schema Management

The following attributes specify the subschema policy and are contained in the subschema subentry and shall be supported:

- dITContentRules
- dITStructureRules
- matchingRules
- attributeTypes
- objectClasses
- nameForms
- matchingRuleUse
- structuralObjectClass
- governingStructureRule

SECTION XINATIONAL DIRECTORY INFORMATION TREES200. Australian DIT

Figure B-3 shows the military portion of the Australian DIT from the top through the first level within the military subtree and the first level of the Army subtree. The remaining subtrees and levels of the military subtree will be shown in the future.

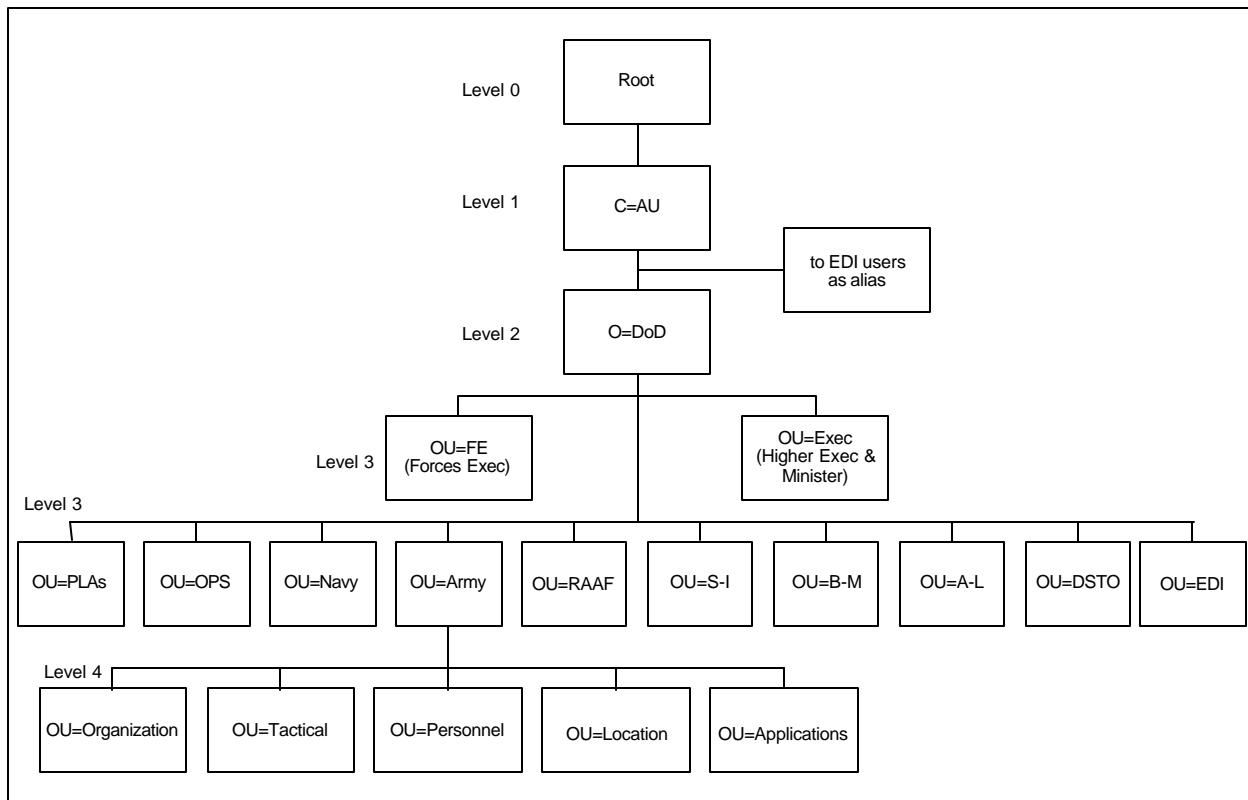


Figure B-3
Australian Top-Level DIT

201. Canadian DIT

Figure B-4 shows the military portion of the Canadian DIT from the top through the beginning of the two military subtrees. The remaining levels of the military subtrees will be shown in the future.

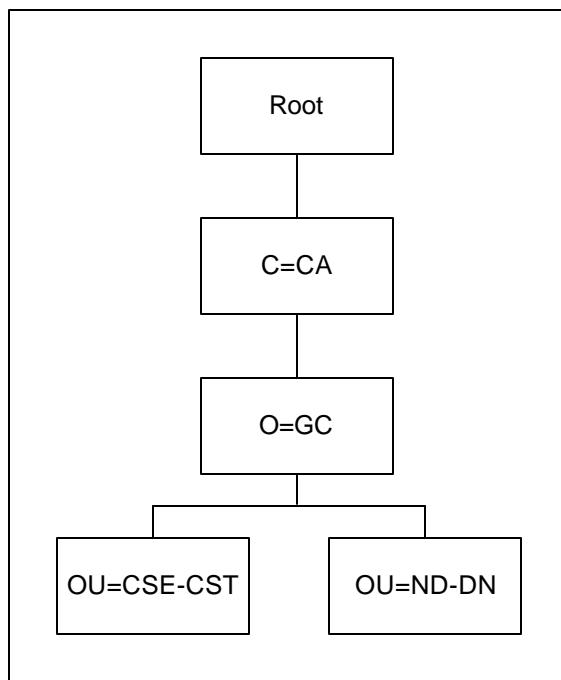


Figure B-4
Canadian Top-Level DIT

202. New Zealand DIT

Figure B-5 shows the military portion of the New Zealand's DIT from the top through the beginning of the (two) military subtrees. The remaining levels of the military subtrees will be shown in the future.

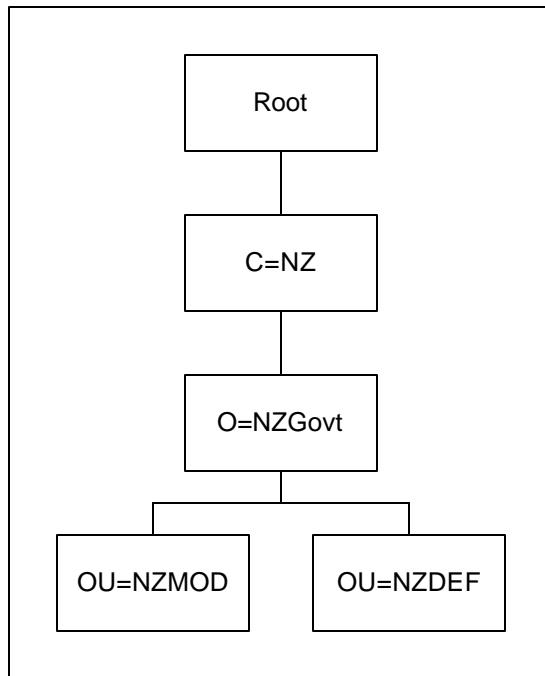


Figure B-5
New Zealand Top-Level DIT

203. United Kingdom DIT

Figure B-6 shows the military portion of the United Kingdom's DIT from the top through the first level within the military subtree. The remaining levels of the military subtree will be shown in the future.

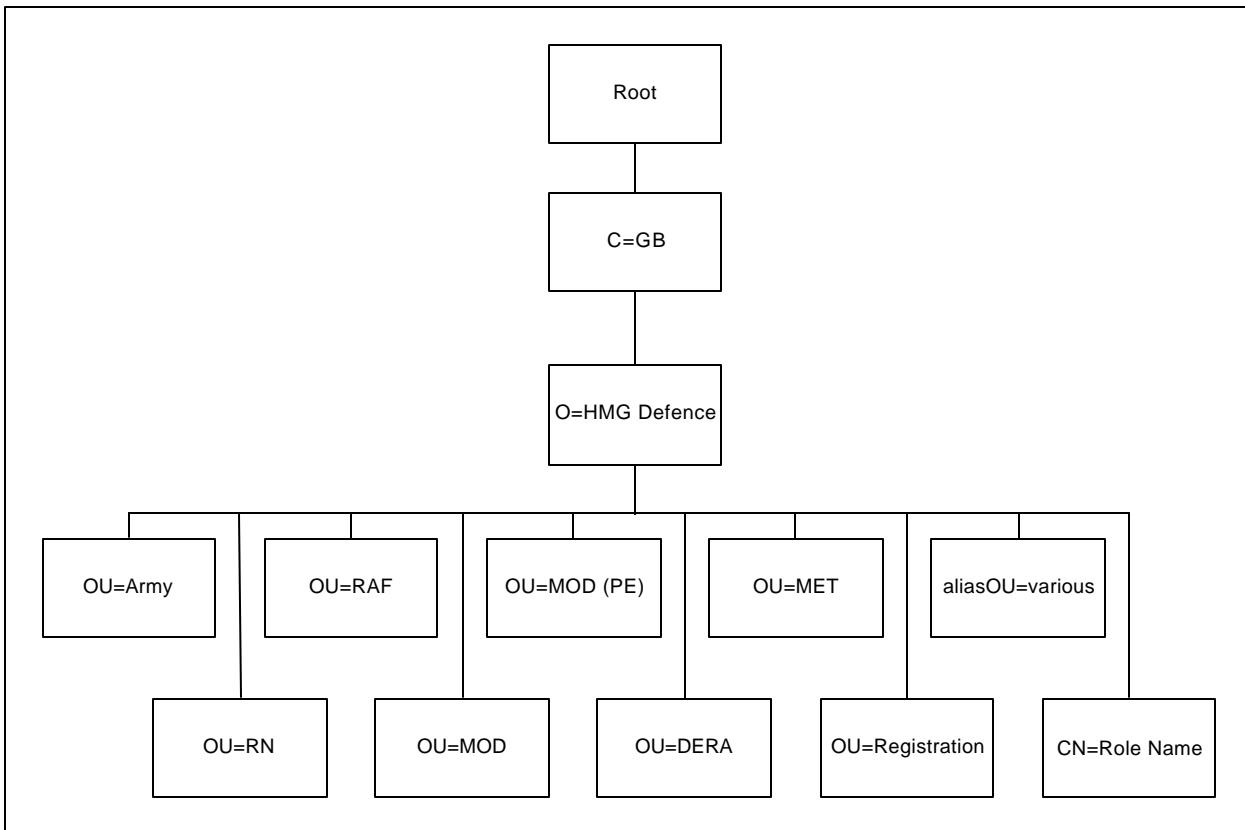


Figure B-6
UK Top-Level DIT

204. United States DITa. Top-Level

Figure B-7 shows the military portion of the United States' DIT from the top through the first level within the military subtree. In the U.S. DIT, the military is represented by an Organizational Unit Ed. B directory (OU=DoD) entry under the Organization Ed. B directory entry that represents the U.S. government. The DoD level is followed by a level that contains an Organizational Unit Ed. B directory entry for each Service, agency, and command.

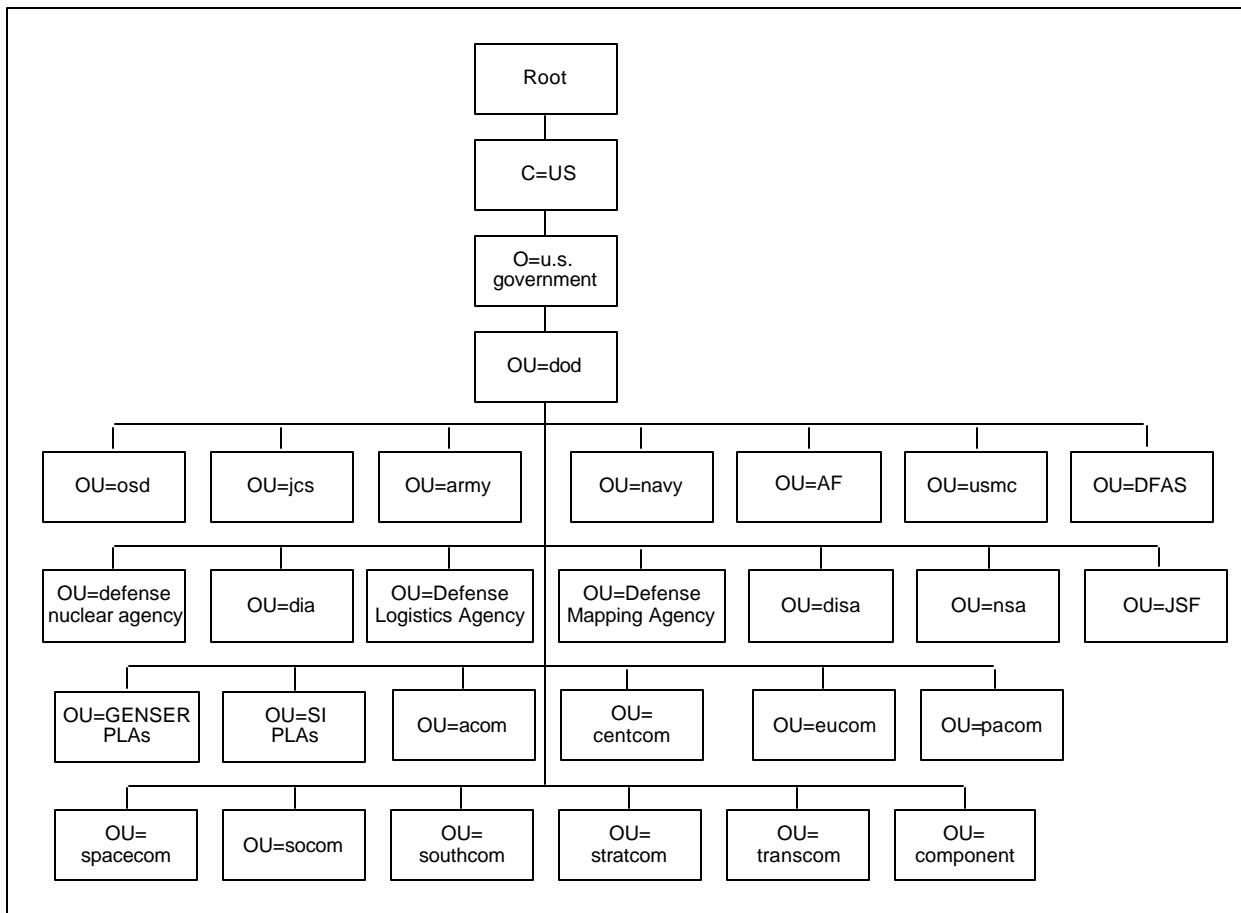


Figure B-7
U.S. Top-Level DIT

b. Service/Agency/Command Subtrees

Under each Service/agency/command directory entry there are at least two subtrees, one for locations, one for organizations, and up to three for special uses appropriate for the

Service/agency/command: ships, address lists, and tactical users. This level is shown in Figure B-8.

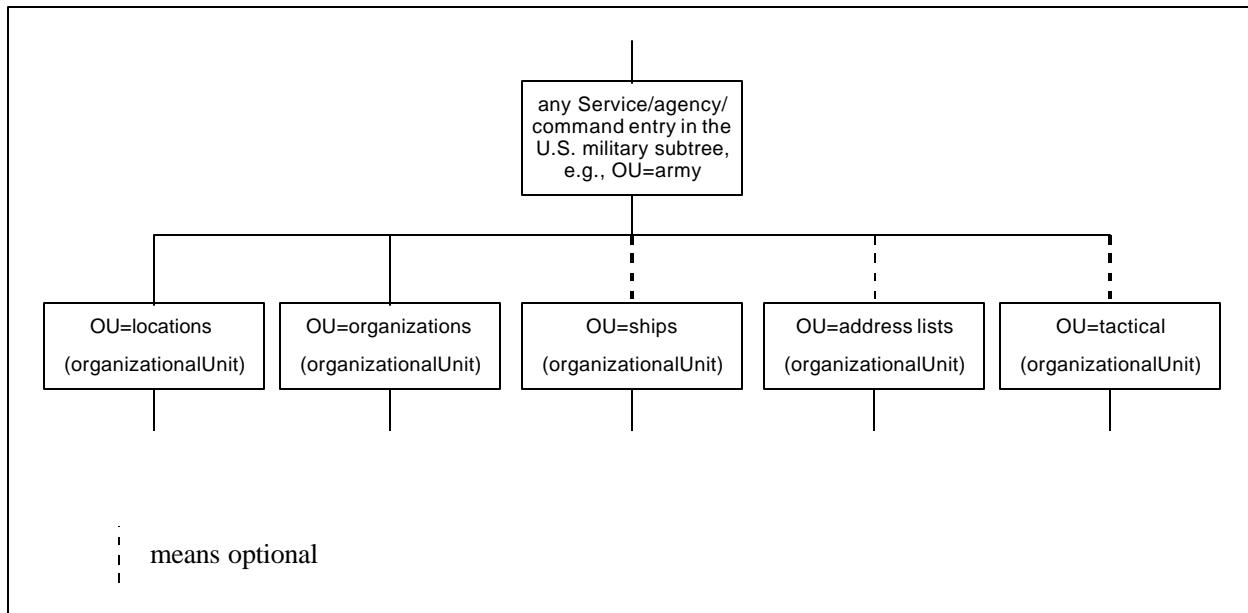


Figure B-8
U.S. DIT Subtrees for Each Service/Agency/Command

(1) Generally, organizational persons will be listed in the locations subtree, shown in Figure B-9, and organizational roles, release authorities, and address lists will be listed in the organizations subtree, shown in Figure B-10. An exception is the role of certification authority which will appear in both locations and organizations subtrees. Aliases for organizational roles may be listed in the locations subtree, and aliases for organizational persons may be listed in the organizational subtree. Devices and application entities may be located in any location or organizational subtree, as appropriate. In the locations subtree, note the optional level of organizational unit. This is used to segment the DIB across multiple DSAs at a site. The organizational subtree also provides for subdivision into localities, if desired.

(2) Figure B-11 and Figure B-12 give examples of the directory entries that could be present in an instance of the locations and organizations subtrees under the Army. Figure B-13 gives examples of the directory entries that could be present in an instance of the locations and organizations subtrees for a combined task force under the Pacific Command (PACOM).

(3) From Figure B-11 and Figure B-12, example Distinguished Names for an individual, a release authority for an organization, and a position in an organization are, respectively:

- { C=US, O=u.s. government, OU=dod, OU=army, OU=locations, L=Fort Huachuca AZ, OU=USAISC, CN=Jones, James R. },
- { C=US, O=u.s. government, OU=dod, OU=army, OU=organizations, OU=DISC4, OU=USAISEC, OU=ASOP-OI, RAN=Jones, James R. }, and
- { C=US, O=u.s. government, OU=dod, OU=army, OU=organizations, OU=DISC4, OU=USAISEC, OU=ASOP-OI, CN=security officer }

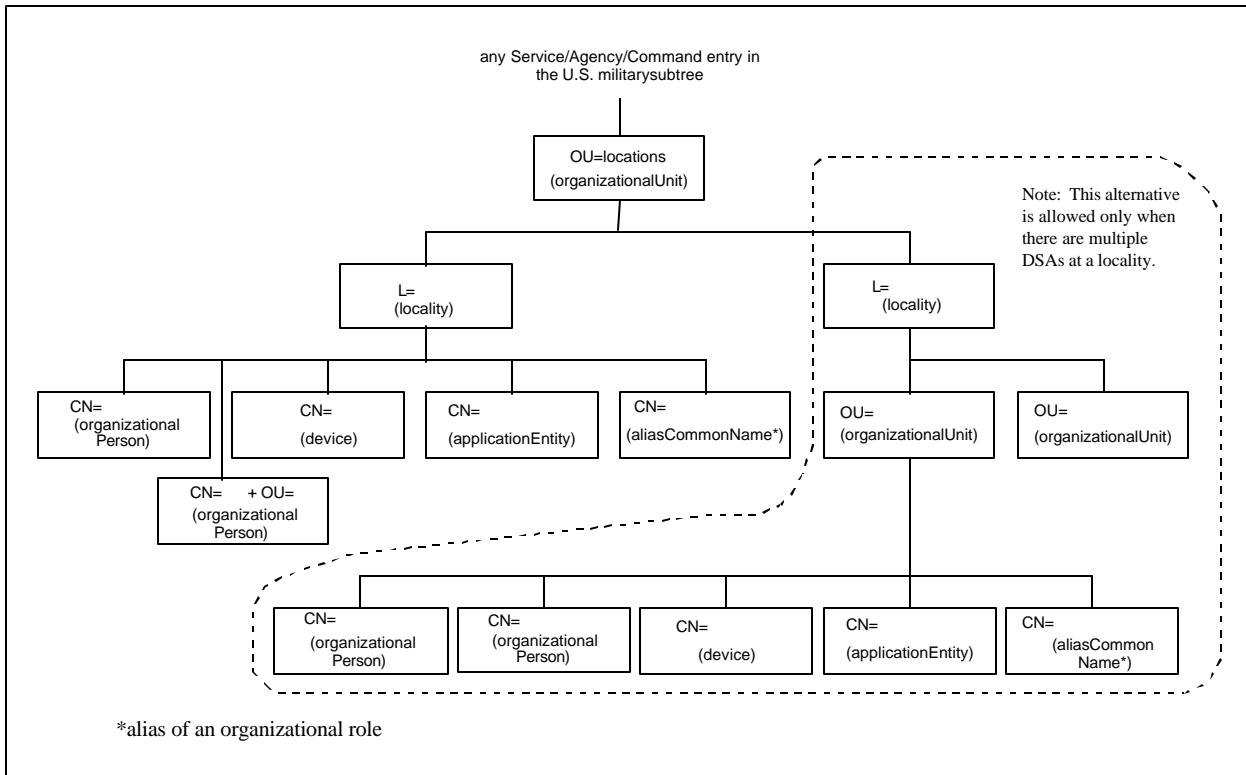


Figure B-9
U.S. DIT Locations Subtree

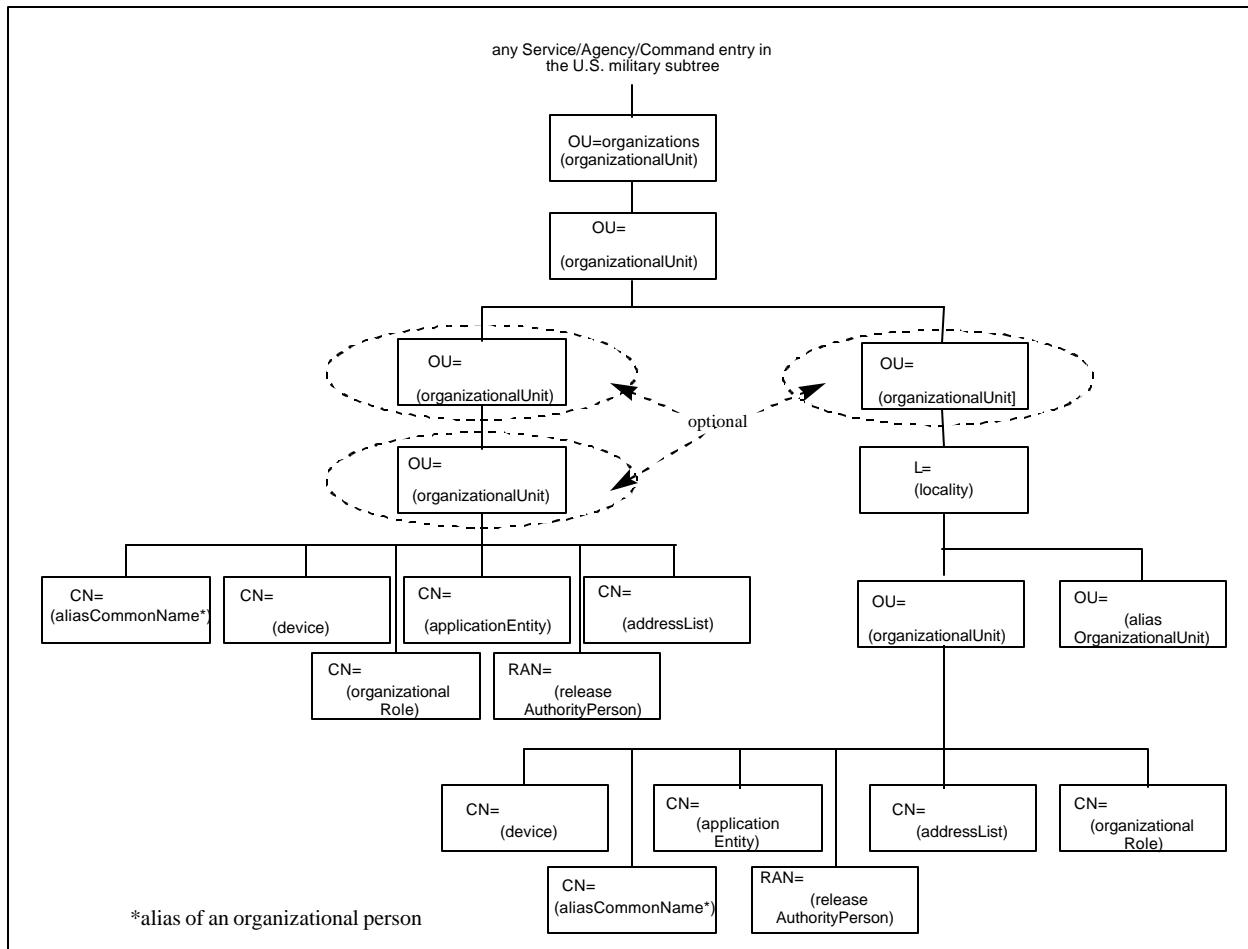


Figure B-10
U.S. DIT Organizations Subtree

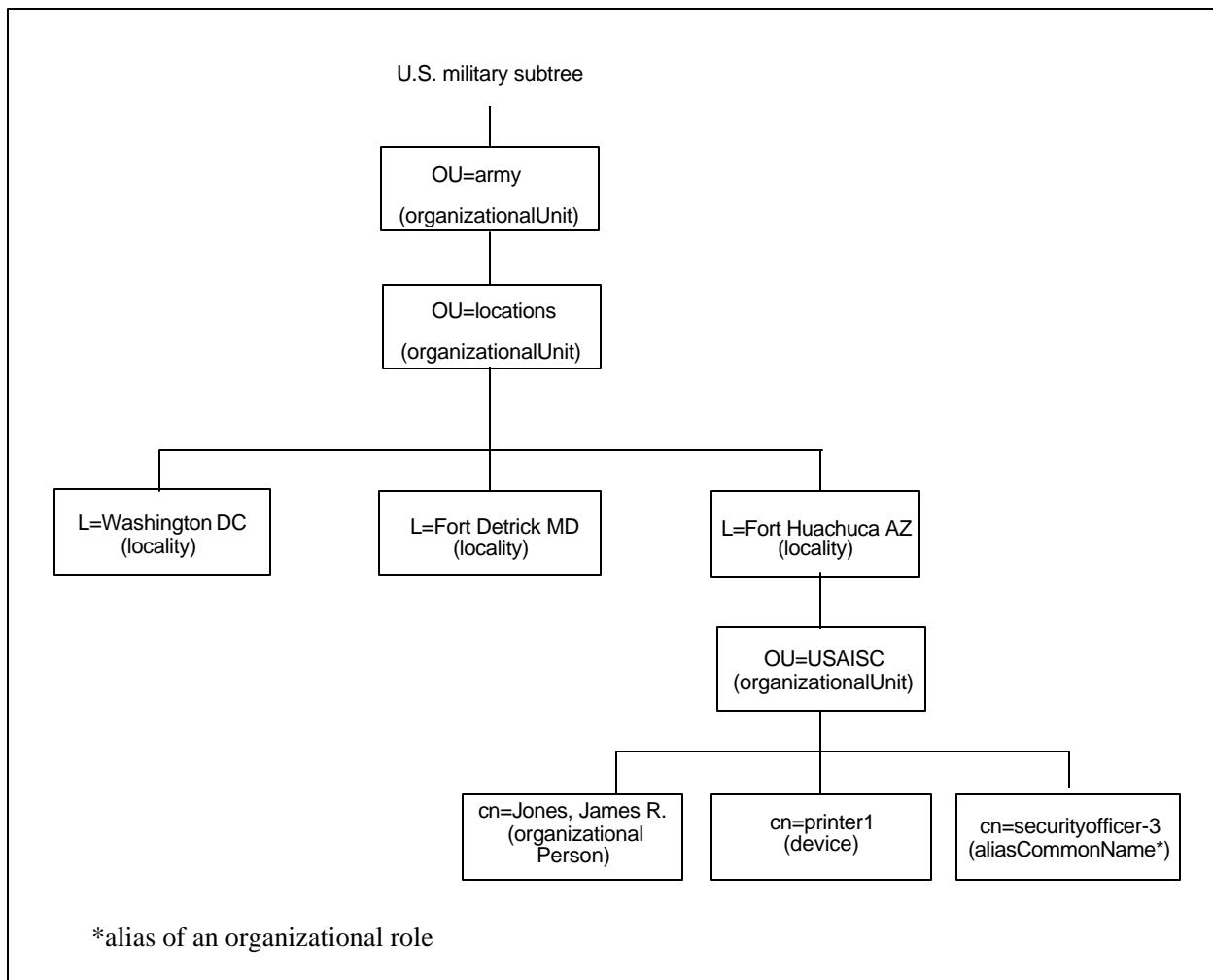


Figure B-11
Example Army Locations Directory Entries

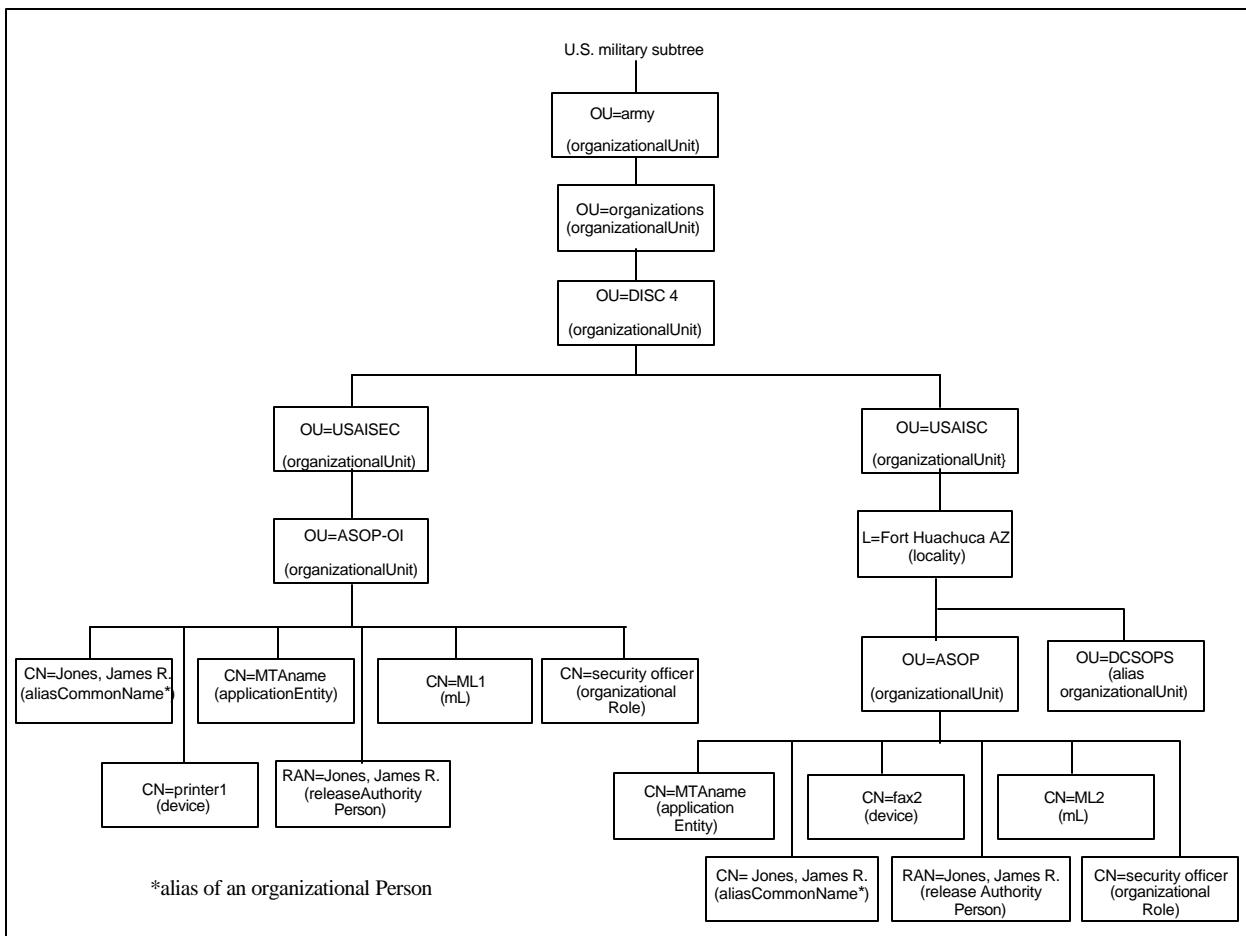


Figure B-12
Example Army Organizations Directory Entries

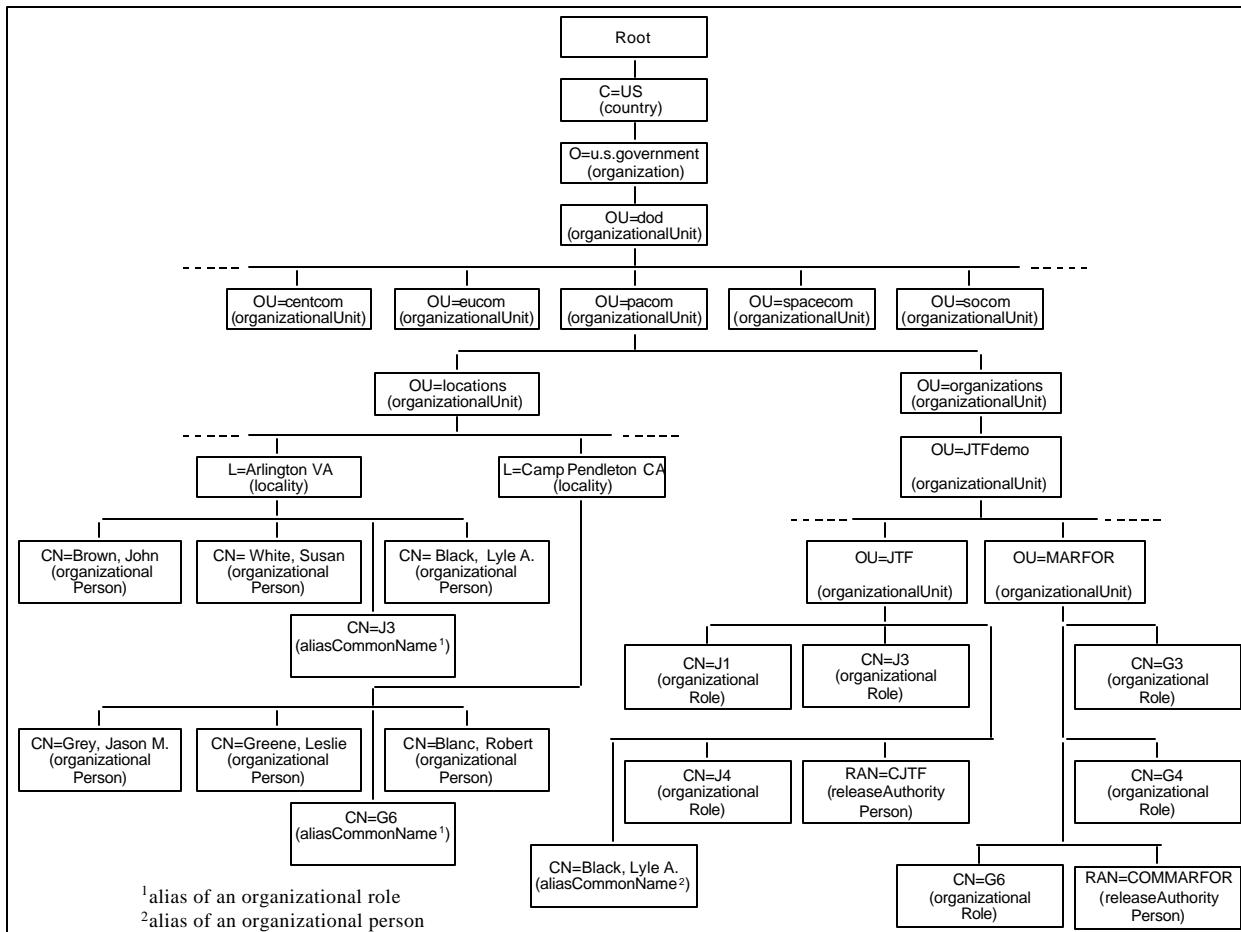


Figure B-13
Example PACOM Combined Task Force Directory Entries

SECTION XII

ACP 133 DATA TYPES

205. Example Content Rules

The following ASN.1 module specifies examples of content rules that realize the combinations given in Table B-54.

ACP133ExampleContentRules { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) module(0) contentRules(4) editionB(3) }

DEFINITIONS ::=

BEGIN

IMPORTS

CONTENT-RULE

FROM InformationFramework {joint-iso-ccitt ds(5) module(1) informationFramework(1) 2 }

businessCategory, dnQualifier

FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) module(1) selectedAttributeTypes(5) 2 }

applicationEntity, cRLDistributionPoint, device, dSA, groupOfNames, locality, organization, organizationalPerson, organizationalRole, organizationalUnit

FROM SelectedObjectClasses { selectedObjectClasses 2 }

 -- Note that the object identifier value of the SelectedObjectClasses

 -- module is not changed by X.521 (1993) Amendment 1

supportedAlgorithms

FROM CertificateExtensions { joint-iso-ccitt ds(5) module(1) certificateExtensions(26) 0 }

pkiCA

FROM AuthenticationFramework {joint-iso-ccitt ds(5) module(1) authenticationFramework(7) 4 }

mhs-distribution-list, mhs-message-store, mhs-message-transfer-agent, mhs-user-agent, mhs-user

FROM MHSDirectoryObjectsAndAttributes { joint-iso-ccitt mhs motis(6) arch(5) modules(0) directory(1) version-1994(0) }

buildingName, rfc822Mailbox

FROM { ccitt data(9) pss(2342) ucl(192003000) pilot(100) pilotAttributeType(1) 3 }

aCPLegacyFormat, addressList, aliasCommonName, aliasOrganizationalUnit, aliasPointer, alternateRecipient, associatedAL, associatedOrganization, associatedPLA, deployed, distributionCodeDescription, distributionCodesHandled, effectiveDate, expirationDate, garrison, guard, listPointer, messagingGateway, mLAgent, nationality, aCPNetworkEdB, aCPNetworkInstructionsEdB, otherContactInformation, plasServed, plaUser, positionNumber, rank, releaseAuthorityPersonA, remarks, routingIndicator, securePkiUser, serviceNumber, sigintPLA, spotPLA, tCCG, ukms

FROM ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) module(0) commonContent(2) editionB (3) }

; -- end of IMPORTS

```

-- a. -- aCPApplicationEntityRuleEdA CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      applicationEntity
   AUXILIARY OBJECT-CLASSES    { pkiCA |
                                 securePkiUser }
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 dnQualifier |
                                 expirationDate
                                 }
 }

-- b. -- aCPCRLDistributionPointRule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      cRLDistributionPoint
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate }
 }

-- c. -- aCPDeviceRuleEdA CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      device
   AUXILIARY OBJECT-CLASSES    { securePkiUser }
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate }
 }

-- d. -- aCPDSARuleEdA CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      dSA
   AUXILIARY OBJECT-CLASSES    { securePkiUser }
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate }
 }

-- e. -- aCPGroupOfNamesRule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      groupOfNames
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate }
 }

```

```

-- f. -- aCPLocalityRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      locality
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

-- g. -- aCPMhs-distribution-listRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      mhs-distribution-list
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

-- h. -- aCPMhs-message-storeRuleEdA CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      mhs-message-store
  AUXILIARY OBJECT-CLASSES    { securePkiUser }
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

-- i. -- aCPMhs-message-transfer-agentRuleEdA CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      mhs-message-transfer-agent
  AUXILIARY OBJECT-CLASSES    { securePkiUser }
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

-- j. -- aCPMhs-user-agentRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      mhs-user-agent
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

```

-- k. -- aCPOrganizationalPersonRuleEdB CONTENT-RULE

```
::= {
  STRUCTURAL OBJECT-CLASS    organizationalPerson
  AUXILIARY OBJECT-CLASSES   { distributionCodesHandled |
                                mhs-user |
                                otherContactInformation |
                                securePkiUser |
                                ukms }

  MAY CONTAIN                { aCPLegacyFormat |
                                aliasPointer |
                                alternateRecipient |
                                businessCategory |
                                deployed |
                                dnQualifier |
                                effectiveDate |
                                expirationDate |
                                garrison |
                                guard |
                                listPointer |
                                nationality |
                                positionNumber |
                                rank |
                                rfc822Mailbox |
                                serviceNumber }

}
```

-- l. -- aCPOrganizationalRoleRuleEdB CONTENT-RULE

```
::= {
  STRUCTURAL OBJECT-CLASS    organizationalRole
  AUXILIARY OBJECT-CLASSES   { pkiCA |
                                distributionCodesHandled |
                                mhs-user |
                                otherContactInformation |
                                securePkiUser |
                                ukms }

  MAY CONTAIN                { aCPLegacyFormat |
                                aliasPointer |
                                alternateRecipient |
                                businessCategory |
                                deployed |
                                dnQualifier |
                                effectiveDate |
                                expirationDate |
                                garrison |
                                guard |
                                listPointer |
                                nationality |
                                rfc822Mailbox }

}
```

```
-- m. -- aCPOrganizationalUnitRuleEdB CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS    organizationalUnit
  AUXILIARY OBJECT-CLASSES   { pkiCA |
                               distributionCodesHandled |
                               mhs-user |
                               otherContactInformation |
                               plaUser |
                               securePkiUser |
                               ukms }

  MAY CONTAIN                { aCPLegacyFormat |
                               aliasPointer |
                               alternateRecipient |
                               associatedPLA |
                               deployed |
                               dnQualifier |
                               effectiveDate |
                               expirationDate |
                               garrison |
                               guard |
                               listPointer |
                               nationality |
                               rfc822Mailbox }

 }
```

```
-- n. -- aCPOrganizationRuleEdB CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS    organization
  AUXILIARY OBJECT-CLASSES   { pkiCA |
                               otherContactInformation }

  MAY CONTAIN                { aCPLegacyFormat |
                               aliasPointer |
                               dnQualifier |
                               effectiveDate |
                               expirationDate }

 }
```

```
-- o. -- aCPRoutingIndicatorRuleEdB CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS    routingIndicator
  MAY CONTAIN                 { tCCG |
                               remarks }

 }
```

```

-- p. -- addressListRuleEdA CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      addressList
  AUXILIARY OBJECT-CLASSES    { distributionCodesHandled |
                                mhs-user |
                                plaUser |
                                securePkiUser |
                                ukms }
MAY CONTAIN                  { aliasPointer |
                                alternateRecipient |
                                effectiveDate |
                                expirationDate |
                                guard |
                                listPointer |
                                rfc822Mailbox }
}

-- q. -- aliasCommonNameRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      aliasCommonName
  MAY CONTAIN                  { effectiveDate |
                                expirationDate }
}

-- r. -- aliasOrganizationalUnitRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      aliasOrganizationalUnit
  MAY CONTAIN                  { effectiveDate |
                                expirationDate }
}

-- s. -- distributionCodeDescriptionRule CONTENT-RULE
 ::= {
  STRUCTURAL OBJECT-CLASS      distributionCodeDescription
  MAY CONTAIN                  { aliasPointer |
                                effectiveDate |
                                expirationDate }
}

```

```
-- t. -- messagingGatewayRuleEdA CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      messagingGateway
   AUXILIARY OBJECT-CLASSES    { securePkiUser |
                                 ukms}
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate |
                                 guard |
                                 plasServed |
                                 rfc822Mailbox }
 }
```

```
-- u. -- mLAgentRule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      mLAgent
   MAY CONTAIN                  { aliasPointer |
                                 effectiveDate |
                                 expirationDate }
 }
```

```
-- v. -- networkEdBRule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      aCPNetworkEdB
   MAY CONTAIN                  { effectiveDate |
                                 expirationDate }
 }
```

```
-- w. -- networkInstructionsEdBRule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      aCPNetworkInstructionsEdB
   MAY CONTAIN                  { effectiveDate |
                                 expirationDate }
 }
```

```
-- x. -- rAPersonRuleEdA CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      releaseAuthorityPersonA
   MAY CONTAIN                  { effectiveDate |
                                 expirationDate }
 }
```

```

-- y. -- sigintPLARule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      sigintPLA
   MAY CONTAIN                  { associatedOrganization }
 }

-- z. -- spotPLARule CONTENT-RULE
 ::= {
   STRUCTURAL OBJECT-CLASS      spotPLA
   MAY CONTAIN                  { associatedAL }
 }

END -- of ACP133ExampleContentRules module

```

206. Common Content ASN.1 Definitions

The following ASN.1 module specifies object classes, attributes, name forms, and other data types for the Allied Directory schema. This module imports only the data types used by the included definitions. That is, data types, that are part of the Common Content but are defined elsewhere and are not used in this module, e.g., the knowledgeInformation attribute, are not imported. Note that some definitions are included that are not used within this module, e.g., the aliasPointer attribute, but are used by the example content rules and are required in the Common Content.

207. Common Content Module

```
ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
dod(2) ds(2) module(0) commonContent(2) editionB (3) }
```

```
DEFINITIONS ::=  
BEGIN
```

IMPORTS

```
alias, ATTRIBUTE, auxiliary, DistinguishedName, distinguishedNameMatch, Name,
```

```
NAME-FORM, OBJECT-CLASS, objectIdentifierMatch, top
```

```
FROM InformationFramework { joint-iso-ccitt ds(5) module(1)  
informationFramework(1) 2 }
```

```
selectedAttributeTypes, selectedObjectClasses, upperBounds
```

```
FROM UsefulDefinitions { joint-iso-ccitt ds(5) module(1) usefulDefinitions(0) 2 }
```

```
attributeCertificate, SIGNED, userCertificate, pkiUser
```

```
FROM AuthenticationFramework { joint-iso-ccitt ds(5) module(1)  
authenticationFramework(7) 4 }
```

```

supportedAlgorithms
  FROM CertificateExtensions { joint-iso-ccitt ds(5) module(1)
                                certificateExtensions(26) 0 }

bitStringMatch, booleanMatch, businessCategory, caseIgnoreListMatch,
caseIgnoreListSubstringsMatch, caseIgnoreMatch, caseIgnoreSubstringsMatch,
commonName, countryName, description, DirectoryString, distinguishedName,
dnQualifier, generalizedTimeMatch, integerMatch, localityName, member, name,
octetStringMatch, organizationalUnitName, organizationName, owner, seeAlso,
stateOrProvinceName, telephoneNumber, telephoneNumberMatch,
telephoneNumberSubstringsMatch,
  FROM SelectedAttributeTypes { selectedAttributeTypes 2 }

applicationEntity, organizationalPerson, strongAuthenticationUser
  FROM SelectedObjectClasses { selectedObjectClasses 2 }

ub-common-name
  FROM UpperBounds upperBounds

mhs-distribution-list, mhs-dl-archive-service, mhs-dl-policy, mhs-dl-related-lists, mhs-dl-
submit-permissions, mhs-dl-subscription-service, mhs-maximum-content-length, mhs-
message-store, mhs-message-transfer-agent, mhs-or-addresses, mhs-user-agent
  FROM MHSDirectoryObjectsAndAttributes { joint-iso-ccitt mhs motis(6) arch(5)
                                           modules(0) directory(1) version-1994(0) }

ORName
  FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                            mts-abstract-service(1) }

Kmid, MLReceiptPolicy, PairwiseTag
  FROM CommonSecurityProtocol { joint-iso-ccitt 16 840 1 101 2 1 id-modules(0)
                               id-csp(16) }

host, roomNumber
  FROM { ccitt data(9) pss(2342) ucl(192003000) pilot(100) pilotAttributeType(1) 3 }

; -- end of IMPORTS

```

-- a. structural object classes

```

-- (1) -- aCPNetworkEdB
 ::= {
   SUBCLASS OF      { top }
   MUST CONTAIN    { commonName }
   MAY CONTAIN     { description |
                      aCPNetworkSchemaEdB |
                      operationName |
                      seeAlso }
   ID              id-oc-aCPNetworkEdB
 }

-- (2) -- aCPNetworkInstructionsEdB OBJECT-CLASS
 ::= {
   SUBCLASS OF    { top }
   MUST CONTAIN  { commonName }
   MAY CONTAIN   { accessCodes |
                      aCPNetwAccessSchemaEdB |
                      description |
                      networkDN }
   ID            id-oc-aCPNetworkInstructionsEdB
 }

-- (3) -- addressList OBJECT-CLASS
 ::= {
   SUBCLASS OF  { top }
   MUST CONTAIN { commonName |
                  mhs-dl-submit-permissions}
   MAY CONTAIN   { businessCategory |
                  copyMember |
                  description |
                  member |
                  mhs-dl-archive-service |
                  mhs-dl-policy |
                  mhs-dl-related-lists |
                  mhs-dl-subscription-service |
                  aLEXemptedAddressProcessor |
                  alid |
                  aLReceiptPolicy |
                  aLType |
                  organizationalUnitName |
                  organizationName |
                  owner |
                  remarks |
                  seeAlso }
   ID          id-oc-addressList
 }
```

```

-- (4) -- aliasCommonName OBJECT-CLASS
 ::= {
   SUBCLASS OF { alias }
   MUST CONTAIN { commonName }
   ID          id-oc-aliasCommonName
 }

-- (5) -- aliasOrganizationalUnit OBJECT-CLASS
 ::= {
   SUBCLASS OF      { alias }
   MUST CONTAIN    { organizationalUnitName }
   ID              id-oc-aliasOrganizationalUnit
 }

-- (6) -- altSpellingACP127 OBJECT-CLASS
 ::= {
   SUBCLASS OF { plaACP127 }
   MUST CONTAIN { plaReplace |
                  primarySpellingACP127 }
   ID          id-oc-altSpellingACP127
 }

-- (7) -- cadACP127.OBJECT-CLASS.
 ::= {
   SUBCLASS OF { plaACP127 }
   MUST CONTAIN { cognizantAuthority}
   MAY CONTAIN  { associatedAL |
                  entryClassification |
                  recapDueDate |
                  rllInfo }
   ID          id-oc-cadACP127
 }

-- (8) -- distributionCodeDescription OBJECT-CLASS
 ::= {
   SUBCLASS OF { top }
   MUST CONTAIN { commonName }
   MAY CONTAIN  { description }
   ID          id-oc-distributionCodeDescription
 }

```

```

-- (9) -- dSSCSPLA OBJECT-CLASS
 ::= {
   SUBCLASS OF      { plaACP127 }
   MUST CONTAIN    { rl }
   MAY CONTAIN     { adminConversion |
                      associatedOrganization |
                      localityName |
                      sigad |
                      usdConversion }
   ID              id-oc-dSSCSPLA
 }

-- (10) -- messagingGateway OBJECT-CLASS
 ::= {
   SUBCLASS OF    { mhs-message-transfer-agent }
   MAY CONTAIN    { administrator |
                      aigsExpanded |
                      gatewayType |
                      ghpType |
                      host |
                      mailDomains |
                      mhs-acceptable-eits |
                      mhs-deliverable-content-types |
                      mhs-exclusively-acceptable-eits |
                      mhs-message-store-dn |
                      mhs-or-addresses |
                      mhs-or-addresses-with-capabilities |
                      mhs-unacceptable-eits |
                      onSupported |
                      plaNameACP127 |
                      rllInfo }
   ID              id-oc-messagingGateway
 }

-- (11) -- mLA OBJECT-CLASS
 ::= {
   SUBCLASS OF    { applicationEntity |
                      strongAuthenticationUser }
   MAY CONTAIN    { supportedAlgorithms}
   ID              id-oc-mLA
 }

```

```
-- (12) -- mAgent OBJECT-CLASS
 ::= {
   SUBCLASS OF { applicationEntity |
                 pkiUser }
   MAY CONTAIN { supportedAlgorithms}
   ID           id-oc-mAgent
 }

-- (13) -- network OBJECT-CLASS
 ::= {
   SUBCLASS OF      { top }
   MUST CONTAIN    { commonName }
   MAY CONTAIN     { description |
                     networkSchema |
                     operationName |
                     seeAlso }
   ID              id-oc-network
 }

-- (14) -- networkInstructions OBJECT-CLASS
 ::= {
   SUBCLASS OF    { top }
   MUST CONTAIN  { commonName }
   MAY CONTAIN   { accessCodes |
                   accessSchema |
                   description |
                   networkDN }
   ID             id-oc-networkInstructions
 }
```

```
-- (15) -- orgACP127 OBJECT-CLASS
 ::= {
   SUBCLASS OF { plaACP127 }
   MAY CONTAIN { accountingCode |
                 associatedOrganization |
                 countryName |
                 dualRoute |
                 entryClassification |
                 localityName |
                 longTitle |
                 minimize |
                 minimizeOverride |
                 nameClassification |
                 rI |
                 rInfo |
                 section |
                 stateOrProvinceName |
                 tARE }
   ID          id-oc-orgACP127
 }
```

```
-- (16) -- plaCollectiveACP127 OBJECT-CLASS
 ::= {
   SUBCLASS OF { plaACP127 }
   MUST CONTAIN { cognizantAuthority }
   MAY CONTAIN { actionAddressees |
                 allowableOriginators |
                 associatedAL |
                 description |
                 entryClassification |
                 infoAddressees |
                 lastRecapDate |
                 recapDueDate }
   ID          id-oc-plaCollectiveACP127
 }
```

```
-- (17) -- releaseAuthorityPerson OBJECT-CLASS
 ::= {
   SUBCLASS OF { secure-user }
   MUST CONTAIN { releaseAuthorityName }
   ID          id-oc-releaseAuthorityPerson
 }
```

```
-- (18) -- releaseAuthorityPersonA OBJECT-CLASS
 ::= {
   SUBCLASS OF { securePkiUser }
   MUST CONTAIN { releaseAuthorityName }
   ID           id-oc-releaseAuthorityPersonA
 }

-- (19) -- routingIndicator OBJECT-CLASS
 ::= {
   SUBCLASS OF { plaData }
   MUST CONTAIN { rl }
   MAY CONTAIN { lmf |
                 mhs-maximum-content-length |
                 nationality |
                 publish |
                 rlClassification |
                 sHD |
                 tCC |
                 transferStation |
                 tRC }
   ID           id-oc-routingIndicator
 }

-- (20) -- sigintPLA OBJECT-CLASS
 ::= {
   SUBCLASS OF { plaData }
   MUST CONTAIN { sigad }
   MAY CONTAIN { localityName |
                 nationality |
                 publish |
                 remarks |
                 rl |
                 shortTitle }
   ID           id-oc-sigintPLA
 }
```

-- (21) -- sIPLA OBJECT-CLASS

```
::= {
  SUBCLASS OF { plaData }
  MUST CONTAIN { longTitle }
  MAY CONTAIN { localityName |
                nationality |
                publish |
                remarks |
                rl |
                shortTitle |
                sigad }
  ID           id-oc-sIPLA
}
```

-- (22) -- spotPLA OBJECT-CLASS

```
::= {
  SUBCLASS OF { plaData }
  MUST CONTAIN { spot }
  MAY CONTAIN { actionAddressees |
                additionalAddressees |
                additionalSecondPartyAddressees |
                mhs-dl-submit-permissions |
                remarks |
                secondPartyAddressees }
  ID           id-oc-spotPLA
}
```

-- (23) -- taskForceACP127 OBJECT-CLASS

```
::= {
  SUBCLASS OF { plaACP127 }
  MUST CONTAIN { cognizantAuthority |
                 lastRecapDate |
                 recapDueDate }
  MAY CONTAIN { associatedAL |
                entryClassification |
                plaAddressees }
  ID           id-oc-taskForceACP127
}
```

-- (24) -- tenantACP127 OBJECT-CLASS

```
::= {
  SUBCLASS OF { plaACP127 }
  MUST CONTAIN { hostOrgACP127 }
  MAY CONTAIN { entryClassification |
                tARE }
  ID           id-oc-tenantACP127
}
```

-- b. auxiliary object classes

```
-- (1) -- distributionCodesHandled OBJECT-CLASS
 ::= {
   SUBCLASS OF {top}
   KIND auxiliary
   MAY CONTAIN { distributionCodeAction |
                 distributionCodeInfo }
   ID           id-oc-distributionCodesHandled
 }
```

```
-- (2) -- otherContactInformation OBJECT-CLASS
 ::= {
   SUBCLASS OF { top }
   KIND auxiliary
   MAY CONTAIN { aCPMobileTelephoneNumber |
                 aCPPagerTelephoneNumber |
                 aCPPREFERREDDelivery |
                 mailDomains |
                 militaryFacsimileNumber |
                 militaryTelephoneNumber |
                 proprietaryMailboxes |
                 roomNumber |
                 secureFacsimileNumber |
                 secureTelephoneNumber }
   ID           id-oc-otherContactInformation
 }
```

```
-- (3) -- plaACP127 OBJECT-CLASS
 ::= {
   SUBCLASS OF { top }
   KIND auxiliary
   MUST CONTAIN { plaNameACP127 }
   MAY CONTAIN { community |
                 effectiveDate |
                 expirationDate |
                 nationality |
                 publish |
                 remarks |
                 serviceOrAgency }
   ID           id-oc-plaACP127
 }
```

-- (4) -- plaData OBJECT-CLASS
 ::= {
 SUBCLASS OF { top }
 KIND auxiliary
 MAY CONTAIN { community |
 description |
 effectiveDate |
 expirationDate }
 ID id-oc-plaData
 }

-- (5) -- plaUser OBJECT-CLASS
 ::= {
 SUBCLASS OF { top }
 KIND auxiliary
 MUST CONTAIN { plaNameACP127 }
 MAY CONTAIN { rInfo }
 ID id-oc-plaUser
 }

-- (6) -- secure-user OBJECT-CLASS
 ::= {
 SUBCLASS OF { strongAuthenticationUser }
 KIND auxiliary
 MAY CONTAIN { attributeCertificate |
 supportedAlgorithms }
 ID id-oc-secure-user
 }

-- (7) -- securePkiUser OBJECT-CLASS
 ::= {
 SUBCLASS OF { pkiUser }
 KIND auxiliary
 MAY CONTAIN { attributeCertificate |
 supportedAlgorithms }
 ID id-oc-securePkiUser
 }

```
-- (8) -- ukms OBJECT-CLASS
 ::= {
   SUBCLASS OF { top }
   KIND auxiliary
   MAY CONTAIN { janUKMs |
                 febUKMs |
                 marUKMs |
                 aprUKMs |
                 mayUKMs |
                 junUKMs |
                 julUKMs |
                 augUKMs |
                 sepUKMs |
                 octUKMs |
                 novUKMs |
                 decUKMs }
   ID          id-oc-ukms
 }
```

-- c. attribute types

```
-- (1) -- accessCodes ATTRIBUTE
 ::= {
   WITH SYNTAX  PrintableString
   ID          id-at-accessCodes
 }

-- (2) -- accessSchema ATTRIBUTE
 ::= {
   WITH SYNTAX  GraphicString
   ID          id-at-accessSchema
 }

-- (3) -- accountingCode ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString (SIZE (1..7))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                      id-at-accountingCode
 }
```

```

-- (4) -- aCPLegacyFormat ATTRIBUTE
::= {
  WITH SYNTAX  ACPLegacyFormat
  SINGLE VALUE TRUE
  ID          id-at-aCPLegacyFormat
}

-- (5) -- aCPMobileTelephoneNumber ATTRIBUTE
::= {
  SUBTYPE OF  telephoneNumber
  ID          id-at-aCPMobileTelephoneNumber
}

-- (6) -- aCPNetwAccessSchemaEdB ATTRIBUTE
::= {
  WITH SYNTAX  JPEG -- values of the string are JPEG- formatted
                  -- (JFIF) photographs
  ID          id-at-aCPNetwAccessSchemaEdB
}

-- (7) -- aCPNetworkSchemaEdB ATTRIBUTE
::= {
  WITH SYNTAX  JPEG -- values of the string are JPEG- formatted
                  -- (JFIF) photographs
  ID          id-at-aCPNetworkSchemaEdB
}

-- (8) -- aCPPagerTelephoneNumber ATTRIBUTE
::= {
  SUBTYPE OF  telephoneNumber
  ID          id-at-aCPPagerTelephoneNumber
}

-- (9) -- aCPPREFERREDDELIVERY ATTRIBUTE
::= {
  WITH SYNTAX  ENUMERATED { SMTP(0), ACP127(1), MHS(2) }
  SINGLE VALUE TRUE
  ID          id-at-aCPPREFERREDDELIVERY
}

```

```

-- (10) -- aCPTelephoneFaxNumber ATTRIBUTE
 ::= {
   WITH SYNTAX          aCPTelephoneFaxNumberSyntax
   EQUALITY MATCHING RULE    telephoneNumberMatch
   SUBSTRINGS MATCHING RULE    telephoneNumberSubstringsMatch
   ID                      id-at-aCPTelephoneFaxNumber
 }

-- (11) -- actionAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE    caseIgnoreListMatch
   SUBSTRINGS MATCHING RULE    caseIgnoreListSubstringsMatch
   ID                      id-at-actionAddressees
 }

-- (12) -- additionalAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE    caseIgnoreListMatch
   SUBSTRINGS MATCHING RULE    caseIgnoreListSubstringsMatch
   ID                      id-at-additionalAddressees
 }

-- (13) -- additionalSecondPartyAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE    caseIgnoreListMatch
   SUBSTRINGS MATCHING RULE    caseIgnoreListSubstringsMatch
   ID                      id-at-additionalSecondPartyAddressees
 }

-- (14) -- adminConversion ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE    caseIgnoreMatch
   SUBSTRING MATCHING RULE    caseIgnoreSubstringsMatch
   ID                      id-at-adminConversion
 }

-- (15) -- administrator ATTRIBUTE
 ::= {
   SUBTYPE OF      distinguishedName
   ID              id-at-administrator
 }

```

```

-- (16) -- aigsExpanded ATTRIBUTE
 ::= {
   SUBTYPE OF  distinguishedName
   ID          id-at-aigsExpanded
 }

-- (17) -- aLExemptedAddressProcessor ATTRIBUTE
 ::= {
   WITH SYNTAX    ORName
   SINGLE VALUE   TRUE
   ID             id-at-aLExemptedAddressProcessor
 }

-- (18) -- aliasPointer ATTRIBUTE
 ::= {
   WITH SYNTAX              DistinguishedName
   EQUALITY MATCHING RULE   distinguishedNameMatch
   ID                       id-at-aliasPointer
 }

-- (19) -- alid ATTRIBUTE
 ::= {
   WITH SYNTAX           Kmid
   EQUALITY MATCHING RULE octetStringMatch
   ID                   id-at-alid
 }

-- (20) -- allowableOriginators ATTRIBUTE
 ::= {
   WITH SYNTAX           Addressees
   EQUALITY MATCHING RULE caselgnoreListMatch
   SUBSTRINGS MATCHING RULE caselgnoreListSubstringsMatch
   ID                   id-at-allowableOriginators
 }

-- (21) -- aLReceiptPolicy ATTRIBUTE
 ::= {
   WITH SYNTAX    MLReceiptPolicy
   SINGLE VALUE   TRUE
   ID             id-at-aLReceiptPolicy
 }

```

```

-- (22) -- alternateRecipient ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE  distinguishedNameMatch
   ID                   id-at-alternateRecipient
 }

-- (23) -- aLType ATTRIBUTE
 ::= {
   WITH SYNTAX          INTEGER { AIG(0), TYPE(1), CAD(2), TASKFORCE(3),
                                     DAG(4) }
   EQUALITY MATCHING RULE  integerMatch
   SINGLE VALUE           TRUE
   ID                     id-at-aLType
 }

-- (24) -- aprUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX    MonthlyUKMs
   SINGLE VALUE   TRUE
   ID             id-at-aprUKMs
 }

-- (25) -- associatedAL ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE  distinguishedNameMatch
   ID                   id-at-associatedAL
 }

-- (26) -- associatedOrganization ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE  distinguishedNameMatch
   ID                   id-at-associatedOrganization
 }

-- (27) -- associatedPLA ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE  distinguishedNameMatch
   ID                   id-at-associatedPLA
 }

```

```

-- (28) -- augUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX  MonthlyUKMs
   SINGLE VALUE TRUE
   ID          id-at-augUKMs
 }

-- (29) -- cognizantAuthority ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString (SIZE (1..55))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                  id-at-cognizantAuthority
 }

-- (30) -- community ATTRIBUTE
 ::= {
   WITH SYNTAX  ENUMERATED { GENSER(0), SI(1), Both(2) }
   SINGLE VALUE TRUE
   ID          id-at-community
 }

-- (31) -- copyMember ATTRIBUTE
 ::= {
   SUBTYPE OF    member
   ID           id-at-copyMember
 }

-- (32) -- decUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX  MonthlyUKMs
   SINGLE VALUE TRUE
   ID          id-at-decUKMs
 }

-- (33) -- deployed ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE distinguishedNameMatch
   ID                  id-at-deployed
 }

```

```

-- (34) -- distributionCodeAction ATTRIBUTE
 ::= {
   WITH SYNTAX          DistributionCode
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-distributionCodeAction
 }

-- (35) -- distributionCodeInfo ATTRIBUTE
 ::= {
   WITH SYNTAX          DistributionCode
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-distributionCodeInfo
 }

-- (36) -- dualRoute ATTRIBUTE
 ::= {
   WITH SYNTAX          BOOLEAN
   EQUALITY MATCHING RULE booleanMatch
   SINGLE VALUE          TRUE
   ID                   id-at-dualRoute
 }

-- (37) -- effectiveDate ATTRIBUTE
 ::= {
   WITH SYNTAX          GeneralizedTime
   EQUALITY MATCHING RULE generalizedTimeMatch
   SINGLE VALUE          TRUE
   ID                   id-at-effectiveDate
 }

-- (38) -- entryClassification ATTRIBUTE
 ::= {
   WITH SYNTAX          Classification
   ID                   id-at-entryClassification
 }

-- (39) -- expirationDate ATTRIBUTE
 ::= {
   WITH SYNTAX          GeneralizedTime
   EQUALITY MATCHING RULE generalizedTimeMatch
   SINGLE VALUE          TRUE
   ID                   id-at-expirationDate
 }

```

```

-- (40) -- febUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX   MonthlyUKMs
   SINGLE VALUE  TRUE
   ID            id-at-febUKMs
 }

-- (41) -- garrison ATTRIBUTE
 ::= {
   WITH SYNTAX           DistinguishedName
   EQUALITY MATCHING RULE distinguishedNameMatch
   ID                   id-at-garrison
 }

-- (42) -- gatewayType ATTRIBUTE
 ::= {
   WITH SYNTAX           OBJECT IDENTIFIER
   EQUALITY MATCHING RULE objectIdentifierMatch
   ID                   id-at-gatewayType
 }

-- (43) -- ghpType ATTRIBUTE
 ::= {
   WITH SYNTAX           OBJECT IDENTIFIER
   EQUALITY MATCHING RULE objectIdentifierMatch
   ID                   id-at-ghpType
 }

-- (44) -- guard ATTRIBUTE
 ::= {
   SUBTYPE OF    distinguishedName
   ID           id-at-guard
 }

-- (45) -- hostOrgACP127 ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString (SIZE (1..55))
   EQUALITY MATCHING RULE caseIgnoreMatch
   SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                   id-at-hostOrgACP127
 }

```

```

-- (46) -- infoAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE caselgnoreListMatch
   SUBSTRINGS MATCHING RULE caselgnoreListSubstringsMatch
   ID                   id-at-infoAddressees
 }

-- (47) -- janUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX      MonthlyUKMs
   SINGLE VALUE    TRUE
   ID              id-at-janUKMs
 }

-- (48) -- julUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX      MonthlyUKMs
   SINGLE VALUE    TRUE
   ID              id-at-julUKMs
 }

-- (49) -- junUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX      MonthlyUKMs
   SINGLE VALUE    TRUE
   ID              id-at-junUKMs
 }

-- (50) -- lastRecapDate ATTRIBUTE
 ::= {
   WITH SYNTAX          GeneralizedTime
   EQUALITY MATCHING RULE generalizedTimeMatch
   SINGLE VALUE         TRUE
   ID                  id-at-lastRecapDate
 }

-- (51) -- listPointer ATTRIBUTE
 ::= {
   WITH SYNTAX          DistinguishedName
   EQUALITY MATCHING RULE distinguishedNameMatch
   ID                  id-at-listPointer
 }

```

```

-- (52) -- lmf ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString (SIZE (1))
   EQUALITY MATCHING RULE caselgnoreMatch
   SINGLE VALUE          TRUE
   ID                   id-at-lmf
 }

-- (53) -- longTitle ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString (SIZE (1...255))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                   id-at-longTitle
 }

-- (54) -- mailDomains ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-mailDomains
 }

-- (55) -- marUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX    MonthlyUKMs
   SINGLE VALUE   TRUE
   ID             id-at-marUKMs
 }

-- (56) -- mayUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX    MonthlyUKMs
   SINGLE VALUE   TRUE
   ID             id-at-mayUKMs
 }

-- (57) -- militaryFacsimileNumber ATTRIBUTE
 ::= {
   SUBTYPE OF    aCPTelephoneFaxNumber
   ID           id-at-militaryFacsimileNumber
 }

```

```

-- (58) -- militaryTelephoneNumber ATTRIBUTE
 ::= {
   SUBTYPE OF    aCPTelephoneFaxNumber
   ID            id-at-militaryTelephoneNumber
 }

-- (59) -- minimize ATTRIBUTE
 ::= {
   WITH SYNTAX      BOOLEAN
 EQUALITY MATCHING RULE  booleanMatch
 SINGLE VALUE        TRUE
 ID                  id-at-minimize
 }

-- (60) -- minimizeOverride ATTRIBUTE
 ::= {
   WITH SYNTAX      BOOLEAN
 EQUALITY MATCHING RULE  booleanMatch
 SINGLE VALUE        TRUE
 ID                  id-at-minimizeOverride
 }

-- (61) -- nameClassification ATTRIBUTE
 ::= {
   WITH SYNTAX    Classification
   ID             id-at-nameClassification
 }

-- (62) -- nationality ATTRIBUTE
 ::= {
   SUBTYPE OF    name
   WITH SYNTAX   PrintableString (SIZE (2)) -- ISO 3166 codes only
   SINGLE VALUE   TRUE
   ID             id-at-nationality
 }

-- (63) -- networkDN ATTRIBUTE
 ::= {
   WITH SYNTAX      DistinguishedName
 EQUALITY MATCHING RULE  distinguishedNameMatch
 ID                  id-at-networkDN
 }

```

```

-- (64) -- networkSchema ATTRIBUTE
 ::= {
   WITH SYNTAX  GraphicString
   ID           id-at-networkSchema
 }

-- (65) -- novUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX  MonthlyUKMs
   SINGLE VALUE TRUE
   ID           id-at-novUKMs
 }

-- (66) -- octUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX  MonthlyUKMs
   SINGLE VALUE TRUE
   ID           id-at-octUKMs
 }

-- (67) -- onSupported ATTRIBUTE
 ::= {
   WITH SYNTAX      BIT STRING { acp127-nn(0), acp127-pn(1), acp127-tn(2) }
   EQUALITY MATCHING RULE  bitStringMatch
   SINGLE VALUE      TRUE
   ID               id-at-onSupported
 }

-- (68) -- operationName ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE  caseIgnoreMatch
   SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
   ID                   id-at-operationName
 }

-- (69) -- plaAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE  caseIgnoreListMatch
   SUBSTRINGS MATCHING RULE  caseIgnoreListSubstringsMatch
   ID                   id-at-plaAddressees
 }

```

```

-- (70) -- plaNameACP127 ATTRIBUTE
 ::= {
   SUBTYPE OFname
   WITH SYNTAX   PrintableString (SIZE (1..55))
   SINGLE VALUE  TRUE
   ID            id-at-plaNameACP127
 }

-- (71) -- plaReplace ATTRIBUTE
 ::= {
   WITH SYNTAX          BOOLEAN
   EQUALITY MATCHING RULE booleanMatch
   SINGLE VALUE         TRUE
   ID                  id-at-plaReplace
 }

-- (72) -- plasServed ATTRIBUTE
 ::= {
   SUBTYPE OF name
   ID           id-at-plasServed
 }

-- (73) -- positionNumber ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-positionNumber
 }

-- (74) -- primarySpellingACP127 ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString (SIZE (1..55))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                   id-at-primarySpellingACP127
 }

-- (75) -- proprietaryMailboxes ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-proprietaryMailboxes
 }

```

```

-- (76) -- publish ATTRIBUTE
 ::= {
   WITH SYNTAX          BOOLEAN
   EQUALITY MATCHING RULE booleanMatch
   SINGLE VALUE          TRUE
   ID                   id-at-publish
 }

-- (77) -- rank ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-rank
 }

-- (78) -- recapDueDate ATTRIBUTE
 ::= {
   WITH SYNTAX          GeneralizedTime
   EQUALITY MATCHING RULE generalizedTimeMatch
   SINGLE VALUE          TRUE
   ID                   id-at-recapDueDate
 }

-- (79) -- releaseAuthorityName ATTRIBUTE
 ::= {
   WITH SYNTAX          DirectoryString (SIZE (1..ub-common-name))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                   id-at-releaseAuthorityName
 }

-- (80) -- remarks ATTRIBUTE
 ::= {
   WITH SYNTAX          Remarks
   EQUALITY MATCHING RULE caselgnoreListMatch
   ID                   id-at-remarks
 }

```

```

-- (81) -- rI ATTRIBUTE
 ::= {
   WITH SYNTAX          PrintableString
   EQUALITY MATCHING RULE    caseIgnoreMatch
   SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
   ID                      id-at-rI
 }

-- (82) -- rIClassification ATTRIBUTE
 ::= {
   WITH SYNTAX      Classification
   ID              id-at-rIClassification
 }

-- (83) -- rInfo ATTRIBUTE
 ::= {
   WITH SYNTAX     RIParameters
   ID              id-at-rInfo
 }

-- (84) -- secondPartyAddressees ATTRIBUTE
 ::= {
   WITH SYNTAX          Addressees
   EQUALITY MATCHING RULE    caseIgnoreListMatch
   SUBSTRINGS MATCHING RULE  caseIgnoreListSubstringsMatch
   ID                      id-at-secondPartyAddressees
 }

-- (85) -- section ATTRIBUTE
 ::= {
   WITH SYNTAX          BOOLEAN
   EQUALITY MATCHING RULE  booleanMatch
   SINGLE VALUE           TRUE
   ID                      id-at-section
 }

-- (86) -- secureFacsimileNumber ATTRIBUTE
 ::= {
   SUBTYPE OF    aCPTelephoneFaxNumber
   ID            id-at-secureFacsimileNumber
 }

```

```

-- (87) -- secureTelephoneNumber ATTRIBUTE
 ::= {
   SUBTYPE OF    aCPTelephoneFaxNumber
   ID            id-at-secureTelephoneNumber
 }

-- (88) -- sepUKMs ATTRIBUTE
 ::= {
   WITH SYNTAX   MonthlyUKMs
   SINGLE VALUE  TRUE
   ID            id-at-sepUKMs
 }

-- (89) -- serviceNumber ATTRIBUTE
 ::= {
   WITH SYNTAX           DirectoryString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                      id-at-serviceNumber
 }

-- (90) -- serviceOrAgency ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                      id-at-serviceOrAgency
 }

-- (91) -- sHD ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   ID                      id-at-sHD
 }

-- (92) -- shortTitle ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString (SIZE (1..55))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE          TRUE
   ID                      id-at-shortTitle
 }

```

```

-- (93) -- sigad ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString (SIZE (5..8))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE            TRUE
   ID                      id-at-sigad
 }

-- (94) -- spot ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString (SIZE (1..55))
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRINGS MATCHING RULE caselgnoreSubstringsMatch
   SINGLE VALUE            TRUE
   ID                      id-at-spot
 }

-- (95) -- tARE ATTRIBUTE
 ::= {
   WITH SYNTAX           BOOLEAN
   EQUALITY MATCHING RULE booleanMatch
   SINGLE VALUE            TRUE
   ID                      id-at-tARE
 }

-- (96) -- tCC ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString
   EQUALITY MATCHING RULE caselgnoreMatch
   SINGLE VALUE            TRUE
   ID                      id-at-tCC
 }

-- (97) -- tCCG ATTRIBUTE
 ::= {
   WITH SYNTAX           PrintableString
   EQUALITY MATCHING RULE caselgnoreMatch
   SUBSTRING MATCHING RULE caselgnoreSubstringsMatch
   ID                      id-at-tCCG
 }

```

-- (98) -- transferStation ATTRIBUTE

```
 ::= {  
   WITH SYNTAX           BOOLEAN  
   EQUALITY MATCHING RULE booleanMatch  
   SINGLE VALUE          TRUE  
   ID                     id-at-transferStation  
 }
```

-- (99) -- tRC ATTRIBUTE

```
 ::= {  
   WITH SYNTAX  
   EQUALITY MATCHING RULE  
   SINGLE VALUE  
   ID  
 }  
   PrintableString  
   caseIgnoreMatch  
   TRUE  
   id-at-tRC
```

-- (100) -- usdConversion ATTRIBUTE

```
::={  
    WITH SYNTAX  
    EQUALITY MATCHING RULE  
    SUBSTRING MATCHING RULE  
    ID  
}  
  
DirectoryString  
caseIgnoreMatch  
caseIgnoreSubstringsMatch  
id-at-usdConversion
```

-- d. collective attributes

-- (1) -- collective-mhs-or-addresses ATTRIBUTE

```
 ::= {  
    SUBTYPE OF mhs-or-addresses  
    ID          id-at-collective-mhs-or-addresses  
}  
}
```

-- (2) -- collectiveMilitaryFacsimileNumber ATTRIBUTE

```
 ::= {  
    SUBTYPE OF    militaryFacsimileNumber  
    ID             id-at-collectiveMilitaryFacsimileNumber  
}
```

-- (3) -- collectiveMilitaryTelephoneNumber ATTRIBUTE

```
 ::= {  
   SUBTYPE OF    militaryTelephoneNumber  
   ID             id-at-collectiveMilitaryTelephoneNumber  
 }
```

```

-- (4) -- collectiveNationality ATTRIBUTE
 ::= {
   SUBTYPE OF  nationality
   ID          id-at-collectiveNationality
 }

-- (5) -- collectiveSecureFacsimileNumber ATTRIBUTE
 ::= {
   SUBTYPE OF  secureFacsimileNumber
   ID          id-at-collectiveSecureFacsimileNumber
 }

-- (6) -- collectiveSecureTelephoneNumber ATTRIBUTE
 ::= {
   SUBTYPE OF  secureTelephoneNumber
   ID          id-at-collectiveSecureTelephoneNumber
 }

-- e. name forms

-- (1) -- aCPNetworkEdBNameForm NAME-FORM
 ::= {
   NAMES          aCPNetworkEdB
   WITH ATTRIBUTES { commonName }
   ID            id-nf-aCPNetworkEdBNameForm
 }

-- (2) -- aCPNetworkInstrEdBNameForm NAME-FORM
 ::= {
   NAMES          aCPNetworkInstructionsEdB
   WITH ATTRIBUTES { commonName }
   ID            id-nf-aCPNetworkInstrEdBNameForm
 }

-- (3) -- addressListNameForm NAME-FORM
 ::= {
   NAMES          addressList
   WITH ATTRIBUTES { commonName }
   ID            id-nf-addressList
 }

```

```

-- (4) -- aENameForm NAME-FORM
 ::= {
   NAMES           applicationEntity
   WITH ATTRIBUTES {commonName}
   AND OPTIONALY  {dnQualifier}
   ID              id-nf-applicationEntityNameForm
 }

-- (5) -- aliasCNNameForm NAME-FORM
 ::= {
   NAMES           { aliasCommonName }
   WITH ATTRIBUTES { commonName }
   ID              id-nf-aliasCNNameForm
 }

-- (6) -- aliasONameForm NAME-FORM
 ::= {
   NAMES           { aliasOrganizationalUnit }
   WITH ATTRIBUTES { organizationalUnitName }
   ID              id-nf-aliasONameForm
 }

-- (7) -- alternateSpellingPLANameForm NAME-FORM
 ::= {
   NAMES           altSpellingACP127
   WITH ATTRIBUTES { plaNameACP127 }
   ID              id-nf-alternateSpellingPLANameForm
 }

-- (8) -- cadPLANameForm NAME-FORM
 ::= {
   NAMES           cadACP127
   WITH ATTRIBUTES {plaNameACP127}
   ID              id-nf-cadPLANameForm
 }

-- (9) -- distributionCodeDescriptionNameForm NAME-FORM
 ::= {
   NAMES           { distributionCodeDescription }
   WITH ATTRIBUTES { commonName }
   ID              id-nf-distributionCodeDescription
 }

```

```

-- (10) -- dSSCSPLANameForm NAME-FORM
 ::= {
   NAMES          dSSCSPLA
   WITH ATTRIBUTES { plaNameACP127 }
   ID             id-nf-dSSCSPLANameForm
 }

-- (11) -- messagingGatewayNameForm NAME-FORM
 ::= {
   NAMES          messagingGateway
   WITH ATTRIBUTES { commonName }
   ID             id-nf-messagingGateway
 }

-- (12) -- mhs-dLNameForm NAME-FORM
 ::= {
   NAMES          mhs-distribution-list
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mhs-dLNameForm
 }

-- (13) -- mLNameForm NAME-FORM
 ::= {
   NAMES          mL
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mLNameForm
 }

-- (14) -- mLAgentNameForm NAME-FORM
 ::= {
   NAMES          mLAgent
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mLAgentNameForm
 }

-- (15) -- mSNameForm NAME-FORM
 ::= {
   NAMES          mhs-message-store
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mS
 }

```

```

-- (16) -- mTANameForm NAME-FORM
 ::= {
   NAMES          mhs-message-transfer-agent
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mTA
 }

-- (17) -- mUANameForm NAME-FORM
 ::= {
   NAMES          mhs-user-agent
   WITH ATTRIBUTES { commonName }
   ID             id-nf-mUA
 }

-- (18) -- networkNameForm NAME-FORM
 ::= {
   NAMES          network
   WITH ATTRIBUTES { commonName }
   ID             id-nf-networkNameForm
 }

-- (19) -- networkInstructionsNameForm NAME-FORM
 ::= {
   NAMES          networkInstructions
   WITH ATTRIBUTES { commonName }
   ID             id-nf-networkInstructionsNameForm
 }

-- (20) -- organizationalPLANameForm NAME-FORM
 ::= {
   NAMES          orgACP127
   WITH ATTRIBUTES { plaNameACP127 }
   ID             id-nf-organizationalPLANameForm
 }

-- (21) -- organizationNameForm NAME-FORM
 ::= {
   NAMES          organization
   WITH ATTRIBUTES {organizationName}
   AND OPTIONALLY {dnQualifier}
   ID             id-nf-qualifiedOrgNameForm
 }

```

```

-- (22) -- orgRNameForm NAME-FORM
 ::= {
   NAMES          organizationalRole
   WITH ATTRIBUTES {commonName}
   AND OPTIONALLY {dnQualifier}
   ID             id-nf-qualifiedOrgRNameForm
 }

-- (23) -- orgUNameForm NAME-FORM
 ::= {
   NAMES          organizationalUnit
   WITH ATTRIBUTES {organizationalUnitName}
   AND OPTIONALLY {dnQualifier}
   ID             id-nf-qualifiedOrgUNameForm
 }

-- (24) -- plaCollectiveNameForm NAME-FORM
 ::= {
   NAMES          plaCollectiveACP127
   WITH ATTRIBUTES { plaNNameACP127 }
   ID             id-nf-plaCollectiveNameForm
 }

-- (25) -- qualifiedOrgPersonNameForm NAME-FORM
 ::= {
   NAMES          organizationalPerson
   WITH ATTRIBUTES {commonName}
   AND OPTIONALLY {dnQualifier | organizationalUnitName}
   ID             id-nf-qualifiedOrgPersonNameForm
 }

-- (26) -- releaseAuthorityPersonNameForm NAME-FORM
 ::= {
   NAMES          releaseAuthorityPerson
   WITH ATTRIBUTES { releaseAuthorityName }
   ID             id-nf-releaseAuthorityPersonNameForm
 }

-- (27) -- releaseAuthorityPersonANameForm NAME-FORM
 ::= {
   NAMES          releaseAuthorityPersonA
   WITH ATTRIBUTES { releaseAuthorityName }
   ID             id-nf-releaseAuthorityPersonANameForm
 }

```

```

-- (28) -- routingIndicatorNameForm NAME-FORM
 ::= {
   NAMES          routingIndicator
   WITH ATTRIBUTES { rl }
   ID             id-nf-routingIndicatorNameForm
 }

-- (29) -- sigintPLANameForm NAME-FORM
 ::= {
   NAMES          sigintPLA
   WITH ATTRIBUTES { sigad }
   ID             id-nf-sigintPLANameForm
 }

-- (30) -- sIPLANameForm NAME-FORM
 ::= {
   NAMES          sIPLA
   WITH ATTRIBUTES { longTitle }
   ID             id-nf-sIPLANameForm
 }

-- (31) -- spotPLANameForm NAME-FORM
 ::= {
   NAMES          spotPLA
   WITH ATTRIBUTES { spot }
   ID             id-nf-spotPLANameForm
 }

-- (32) -- taskForcePLANameForm NAME-FORM
 ::= {
   NAMES          taskForceACP127
   WITH ATTRIBUTES { plaNameACP127 }
   ID             id-nf-taskForcePLANameForm
 }

-- (33) -- tenantPLANameForm NAME-FORM
 ::= {
   NAMES          tenantACP127
   WITH ATTRIBUTES { plaNameACP127 }
   ID             id-nf-tenantPLANameForm
 }

```

```
-- superseded name form
-- uniqueOrgPersonNameForm NAME-FORM
-- ::= {
-- NAMES          organizationalPerson
-- WITH ATTRIBUTES { commonName }
-- AND OPTIONALLY { organizationalUnitName |
--                   uniquelIdentifier }
-- ID             id-nf-uniqueOrgPersonNameForm
-- }
```

-- f. miscellaneous data types

```
ACPLegacyFormat ::= INTEGER {
                           JANAP128(0),
                           ACP126(1),
                           DOI103(2),
                           DOI103Special(3),
                           ACP127(4),
                           ACP127Converted(5),
                           Reserved1(6),      -- hold for ACP127Standard if
                           -- needed
                           ACP127State(7),
                           ACP127Modified(8),
                           SOCOMMSSpecial(9),
                           SOCOMMNarrative(10),
                           Reserved2(11),     -- hold for SOCOMMNarrativeTTY if
                           -- needed
                           SOCOMMNarrativeSpecial(12),
                           SOCOMMData(13),
                           SOCOMMInternal(14),
                           SOCOMMEExternal(15) }
                           -- Note: Values 32 through 48 are not defined
                           -- by this ACP and may be used nationally or
                           -- bilaterally.
```

ACPTelephoneFaxNumberSyntax ::= PrintableString -- constructed as defined in
-- paragraph 27 in this annex

Addressees ::= SEQUENCE OF PrintableString (SIZE (1..55))

Classification ::= ENUMERATED { unmarked(0), unclassified(1), restricted(2),
confidential(3), secret(4), top-secret(5) }

DistributionCode ::= PrintableString

JPEG ::= OCTET STRING -- a JPEG image

MonthlyUKMs ::= SIGNED { SEQUENCE OF UKMEntry }

Remarks ::= SEQUENCE OF PrintableString

```

RIParameters ::= SET {
    rl          [0] PrintableString,
    rType       [1] ENUMERATED { normal(0), off-line(1), partTimeTerminal(2) },
    minimize    [2] BOOLEAN, -- not used any more --
    sHD         [3] PrintableString,
    classification [4] Classification
}

```

```

UKMEntry ::= SEQUENCE {
    tag      PairwiseTag,
    ukm     OCTET STRING
}

```

-- g. object identifiers

ID ::= OBJECT IDENTIFIER

ds ID ::= { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) }

--categories of information objects--

```

id-module   ID ::= {id-ds 0}
id-attributeType ID ::= {id-ds 1}
id-objectClass  ID ::= {id-ds 3}
id-nameForm    ID ::= {id-ds 4}
id-gatewayType ID ::= {id-ds 5 }

```

-- synonyms --

```

id-at    ID ::= { id-ds attributeType(1) }
id-gt    ID ::= { id-ds gatewayType(5) }
id-nf    ID ::= { id-ds nameForm(4) }
id-oc    ID ::= { id-ds objectClass(3) }

```

-- Attributes registered in SDN.700 , which is the definitive assignment, and
-- repeated here

```

id-at-alid -- [id-mlid] -- ID ::= { 2 16 840 1 101 2 1 5 14 }
id-at-janUKMs  ID ::= { 2 16 840 1 101 2 1 5 20 }
id-at-febUKMs ID ::= { 2 16 840 1 101 2 1 5 21 }
id-at-marUKMs ID ::= { 2 16 840 1 101 2 1 5 22 }
id-at-aprUKMs ID ::= { 2 16 840 1 101 2 1 5 23 }
id-at-mayUKMs ID ::= { 2 16 840 1 101 2 1 5 24 }
id-at-junUKMs ID ::= { 2 16 840 1 101 2 1 5 25 }
id-at-julUKMs ID ::= { 2 16 840 1 101 2 1 5 26 }
id-at-augUKMs ID ::= { 2 16 840 1 101 2 1 5 27 }
id-at-sepUKMs ID ::= { 2 16 840 1 101 2 1 5 28 }
id-at-octUKMs ID ::= { 2 16 840 1 101 2 1 5 29 }
id-at-novUKMs ID ::= { 2 16 840 1 101 2 1 5 30 }

```

id-at-decUKMs ID ::= { 2 16 840 1 101 2 1 5 31 }
id-at-aLExemptedAddressProcessor ID ::= { 2 16 840 1 101 2 1 5 47 }
-- [id-mIExemptedAddressProcessor]

-- Attributes registered in RFC 1274 --

-- buildingName ID ::= { 0 9 2342 192003000 100 1 48 } --
-- host ID ::= { 0 9 2342 192003000 100 1 9 } --
-- rfc822Mailbox ID ::= { 0 9 2342 192003000 100 1 3 } --
-- roomNumber ID ::= { 0 9 2342 192003000 100 1 6 } --

-- ACP 133 attributes --

id-at-alternateRecipient ID ::= { id-at 3 }
id-at-associatedOrganization ID ::= { id-at 4 }
id-at-associatedPLA ID ::= { id-at 6 }
id-at-releaseAuthorityName ID ::= { id-at 45 }
id-at-actionAddressees ID ::= { id-at 46 }
id-at-additionalAddressees ID ::= { id-at 47 }
id-at-additionalSecondPartyAddressees ID ::= { id-at 48 }
id-at-aliasPointer ID ::= { id-at 49 }
id-at-allowableOriginators ID ::= { id-at 50 }
id-at-cognizantAuthority ID ::= { id-at 51 }
id-at-community ID ::= { id-at 52 }
id-at-accountingCode ID ::= { id-at 53 }
id-at-dualRoute ID ::= { id-at 54 }
id-at-effectiveDate ID ::= { id-at 55 }
id-at-entryClassification ID ::= { id-at 56 }
id-at-expirationDate ID ::= { id-at 57 }
id-at-hostOrgACP127 ID ::= { id-at 58 }
id-at-infoAddressees ID ::= { id-at 59 }
id-at-lastRecapDate ID ::= { id-at 60 }
id-at-listPointer ID ::= { id-at 61 }
id-at-lmf ID ::= { id-at 62 }
id-at-longTitle ID ::= { id-at 63 }
id-at-minimize ID ::= { id-at 64 }
id-at-minimizeOverride ID ::= { id-at 65 }
id-at-nameClassification ID ::= { id-at 67 }
id-at-nationality ID ::= { id-at 68 }
id-at-collectiveNationality ID ::= { id-at 68 collective(1) }
id-at-transferStation ID ::= { id-at 69 }
id-at-plaNameACP127 ID ::= { id-at 70 }
id-at-plaAddressees ID ::= { id-at 71 }
id-at-plaReplace ID ::= { id-at 72 }
id-at-primarySpellingACP127 ID ::= { id-at 73 }
id-at-publish ID ::= { id-at 74 }
id-at-recapDueDate ID ::= { id-at 75 }
id-at-remarks ID ::= { id-at 76 }
id-at-rl ID ::= { id-at 77 }
id-at-rlClassification ID ::= { id-at 78 }
id-at-rlInfo ID ::= { id-at 79 }

id-at-secondPartyAddressees ID ::= { id-at 80 }
 id-at-section ID ::= { id-at 81 }
 id-at-serviceOrAgency ID ::= { id-at 82 }
 id-at-sHD ID ::= { id-at 83 }
 id-at-shortTitle ID ::= { id-at 84 }
 id-at-sigad ID ::= { id-at 85 }
 id-at-spot ID ::= { id-at 86 }
 id-at-tARE ID ::= { id-at 87 }
 id-at-aCPMobileTelephoneNumber ID ::= { id-at 94 }
 id-at-aCPPagerTelephoneNumber ID ::= { id-at 95 }
 id-at-tCC ID ::= { id-at 96 }
 id-at-tRC ID ::= { id-at 97 }
 id-at-distributionCodeAction ID ::= { id-at 104 }
 id-at-distributionCodeInfo ID ::= { id-at 105 }
 id-at-accessCodes ID ::= { id-at 106 }
 id-at-accessSchema ID ::= { id-at 107 }
 id-at-aCPPREFERREDDelivery ID ::= { id-at 108 }
 id-at-aCPTelephoneFaxNumber ID ::= { id-at 109 }
 id-at-administrator ID ::= { id-at 110 }
 id-at-aigsExpanded ID ::= { id-at 111 }
 id-at-aLType ID ::= { id-at 112 }
 id-at-associatedAL ID ::= { id-at 113 }
 id-at-copyMember ID ::= { id-at 114 }
 id-at-gatewayType ID ::= { id-at 115 }
 id-at-ghpType ID ::= { id-at 116 }
 id-at-guard ID ::= { id-at 117 }
 id-at-mailDomains ID ::= { id-at 118 }
 id-at-militaryFacsimileNumber ID ::= { id-at 119 }
 id-at-collectiveMilitaryFacsimileNumber ID ::= { id-at 119 collective(1) }
 id-at-militaryTelephoneNumber ID ::= { id-at 120 }
 id-at-collectiveMilitaryTelephoneNumber ID ::= { id-at 120 collective(1) }
 id-at-networkDN ID ::= { id-at 121 }
 id-at-networkSchema ID ::= { id-at 122 }
 id-at-onSupported ID ::= { id-at 123 }
 id-at-operationName ID ::= { id-at 124 }
 id-at-positionNumber ID ::= { id-at 125 }
 id-at-proprietaryMailboxes ID ::= { id-at 126 }
 id-at-secureFacsimileNumber ID ::= { id-at 127 }
 id-at-collectiveSecureFacsimileNumber ID ::= { id-at 127 collective(1) }
 id-at-secureTelephoneNumber ID ::= { id-at 128 }
 id-at-collectiveSecureTelephoneNumber ID ::= { id-at 128 collective(1) }
 id-at-serviceNumberID ::= { id-at 129 }
 id-at-rank ID ::= { id-at 133 }
 id-at-misc-collectives ID ::= { id-at 134 }
 id-at-collective-mhs-or-addresses ID ::= { id-at 134 collective-mhs-or-addresses(1) }
 id-at-aLReceiptPolicy ID ::= { id-at 135 }
 id-at-plasServed ID ::= { id-at 138 }
 id-at-deployed ID ::= { id-at 139 }
 id-at-garrisonID ::= { id-at 140 }
 id-at-aCPLegacyFormat ID ::= { id-at 142 }
 id-at-adminConversion ID ::= { id-at 143 }

id-at-tCCG ID ::= { id-at 144 }
id-at-usdConversionID ::= { id-at 145 }
id-at-aCPNetwAccessSchemaEdB ID ::= { id-at 146 }
id-at-aCPNetworkSchemaEdB ID ::= { id-at 147 }

-- ACP 133 Name Forms --

id-nf-alternateSpellingPLANameForm ID ::= { id-nf 4 }
id-nf-cadPLANameForm ID ::= { id-nf 6 }
id-nf-mLANameForm ID ::= { id-nf 9 }
id-nf-organizationalPLANameForm ID ::= { id-nf 12 }
id-nf-plaCollectiveNameForm ID ::= { id-nf 13 }
id-nf-routingIndicatorNameForm ID ::= { id-nf 15 }
id-nf-sigintPLANameForm ID ::= { id-nf 16 }
id-nf-sIPLANameForm ID ::= { id-nf 17 }
id-nf-spotPLANameForm ID ::= { id-nf 18 }
id-nf-taskForcePLANameForm ID ::= { id-nf 19 }
id-nf-tenantPLANameForm ID ::= { id-nf 20 }
id-nf-aliasCNNameForm ID ::= { id-nf 21 }
id-nf-aliasOONameForm ID ::= { id-nf 22 }
id-nf-distributionCodeDescription ID ::= { id-nf 23 }
id-nf-mS ID ::= { id-nf 24 }
id-nf-mTA ID ::= { id-nf 25 }
id-nf-mUA ID ::= { id-nf 26 }
id-nf-addressList ID ::= { id-nf 27 }
id-nf-messagingGateway ID ::= { id-nf 28 }
id-nf-mhs-dLNameForm ID ::= { id-nf 29 }
id-nf-networkNameForm ID ::= { id-nf 30 }
id-nf-networkInstructionsNameForm ID ::= { id-nf 31 }
id-nf-releaseAuthorityPersonNameForm ID ::= { id-nf 32 }
-- **id-nf-uniqueOrgPersonNameForm** ID ::= { id-nf 33 } (superseded)
id-nf-applicationEntityNameForm ID ::= { id-nf 34 }
id-nf-qualifiedOrgNameForm ID ::= { id-nf 35 }
id-nf-qualifiedOrgPersonNameForm ID ::= { id-nf 36 }
id-nf-qualifiedOrgRNameForm ID ::= { id-nf 37 }
id-nf-qualifiedOrgUNameForm ID ::= { id-nf 38 }
id-nf-releaseAuthorityPersonANameForm ID ::= { id-nf 39 }
id-nf-mLAgentNameForm ID ::= { id-nf 40 }
id-nf-dSSCSPLANameFormID ::= { id-nf 41 }
id-nf-aCPNetworkEdBNameForm ID ::= { id-nf 42 }
id-nf-aCPNetworkInstrEdBNameFormID ::= { id-nf 43 }

-- Object classes registered in SDN.700 , which is the definitive assignment,
-- and repeated here

id-oc-secure-user ID ::= { 2 16 840 1 101 2 1 4 13 }
id-oc-ukms ID ::= { 2 16 840 1 101 2 1 4 16 }

-- ACP 133 object classes --

```

id-oc-plaData    ID ::= { id-oc 26 }
id-oc-cadACP127 ID ::= { id-oc 28 }
id-oc-mLA      ID ::= { id-oc 31 }
id-oc-orgACP127 ID ::= { id-oc 34 }
id-oc-plaCollectiveACP127 ID ::= { id-oc 35 }
id-oc-routingIndicator ID ::= { id-oc 37 }
id-oc-sigintPLA  ID ::= { id-oc 38 }
id-oc-sIPLA     ID ::= { id-oc 39 }
id-oc-spotPLA   ID ::= { id-oc 40 }
id-oc-taskForceACP127 ID ::= { id-oc 41 }
id-oc-tenantACP127 ID ::= { id-oc 42 }
id-oc-plaACP127 ID ::= { id-oc 47 }
id-oc-aliasCommonName ID ::= { id-oc 52 }
id-oc-aliasOrganizationalUnit ID ::= { id-oc 53 }
id-oc-distributionCodesHandled ID ::= { id-oc 54 }
id-oc-distributionCodeDescription ID ::= { id-oc 55 }
id-oc-plaUser    ID ::= { id-oc 56 }
id-oc-addressList ID ::= { id-oc 57 }
id-oc-altSpellingACP127 ID ::= { id-oc 58 }
id-oc-messagingGateway ID ::= { id-oc 59 }
id-oc-network    ID ::= { id-oc 60 }
id-oc-networkInstructions ID ::= { id-oc 61 }
id-oc-otherContactInformation ID ::= { id-oc 62 }
id-oc-releaseAuthorityPerson ID ::= { id-oc 63 }
id-oc-mLAgent    ID ::= { id-oc 64 }
id-oc-releaseAuthorityPersonAID ::= { id-oc 65 }
id-oc-securePkiUserID ::= { id-oc 66 }
id-oc-dSSCSPLAID ::= { id-oc 67 }
id-oc-aCPNetworkEdB ID ::= { id-oc 68 }
id-oc-aCPNetworkInstructionsEdBID ::= { id-oc 69 }

```

--gateway types--

```

acp120-acp127  ID ::= { id-gt 0 }
acp120-janap128 ID ::= { id-gt 1 }
acp120-mhs     ID ::= { id-gt 2 }
acp120-mmhs    ID ::= { id-gt 3 }
acp120-rfc822  ID ::= { id-gt 4 }
boundaryMTA    ID ::= { id-gt 5 }
mmhs-mhs      ID ::= { id-gt 6 }
mmhs-rfc822  ID ::= { id-gt 7 }
mta-acp127    ID ::= { id-gt 8 }

```

END -- Common Content --

208. Useful Attributes ASN.1 Definitions

The following ASN.1 module specifies attributes and their object identifiers that are useful to more than one of the Allies, but are not part of the Allied Directory schema. This module imports only the data types used by the included definitions. Useful attributes shall not be replicated unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

209. Useful Attributes Module

ACP133UsefulAttributes { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) module(0) usefulAttributes(3) editionA(2) }

DEFINITIONS ::=

BEGIN

IMPORTS

ATTRIBUTE

FROM InformationFramework { joint-iso-ccitt ds(5) modules(1) informationFramework(1) 2 }

caseignoreMatch, caseignoreSubstringsMatch, DirectoryString, postalAddress
FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) module(1) usefulDefinitions(0) 2 }

id-at, JPEG

FROM ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) module(0) 2 2 }

; -- end of IMPORTS

-- a. -- hoursOfOperation ATTRIBUTE

```
::= {
  WITH SYNTAX DirectoryString
  EQUALITY MATCHING RULE caseignoreMatch
  SUBSTRINGS MATCHING RULE caseignoreSubstringsMatch
  ID id-at-hoursOfOperation
}
```

-- b. -- jpegPhoto ATTRIBUTE

```
::= {
  WITH SYNTAX OCTET STRINGJPEG -- values of the string are
                                -- JPEG- formatted (JFIF) photographs
  ID id-at-jpegPhoto
}
```

```

-- c. -- militaryPostalAddress ATTRIBUTE
 ::= {
   SUBTYPE OF          postalAddress
   ID                  id-at-militaryPostalAddress
 }

-- d. -- visitorAddress ATTRIBUTE
 ::= {
   SUBTYPE OF          postalAddress
   ID                  id-at-visitorAddress
 }

-- e. -- collectiveMilitaryPostalAddress ATTRIBUTE
 ::= {
   SUBTYPE OF          militaryPostalAddress
   ID                  id-at-collectiveMilitaryPostalAddress
 }

-- f. -- collectiveVisitorAddress ATTRIBUTE
 ::= {
   SUBTYPE OF          visitorAddress
   ID                  id-at-collectiveVisitorAddress
 }

id-at-hoursOfOperation ID ::= { id-at 130 }
id-at-jpegPhoto ID ::= { 0 9 2342 19200300 100 1 60 }
id-at-militaryPostalAddressID ::= { id-at 131 }
id-at-collectiveMilitaryPostalAddress ID ::= { id-at 131 collective(1) }
id-at-visitorAddress ID ::= { id-at 132 }
id-at-collectiveVisitorAddress ID ::= { id-at 132 collective(1) }

```

END -- Useful Attributes --

